はじめよう数学

上野健爾|浪川幸彦|高橋陽一郎|編集

4

数論の3つの真珠

A.Y.Khinchin

ア・ヤ・ヒンチン

[著]

Kanie Yukihiro

蟹江幸博

[訳・解説]

日本評論社

TRI ZHEMCHUZNYE TEORII CHISEL

by

A.IA.KHINCHIN

はじめよう数学

この本を手に取られたみなさん！

この本は，同じシリーズの他の本とともに，みなさんを新しい数学の世界に御案内します．

出発地は，みなさんが大学や高等学校で学んでいる数学そのものです．いえ，ここで本を閉じてはいけません．みなさんの学んでいる数学が，いかに豊かでさまざまな数学の世界につながっているかを具体的に知っていただこうというのがこのシリーズの目的です．

旅行の準備として用意していただくものは鉛筆と紙．必ず自分で計算したり，図を書いたりして，自分の頭で考えながらお読みください．結構ハードな道もありますから，寝転がって読んでいたりすると，道に迷ってしまうかも知れませんよ．

私達がみなさんをお連れしようとしている場所は様々です．

数学は数千年以上昔，エジプト，メソポタミアで生まれ，ギリシャで一つの「学問」になりました．ピタゴラスやユークリッドの世界です．ある本はそうした数学の古い伝統がいかに現代にまで連なっているかを見せてくれるでしょう．

近代数学は，18 世紀のオイラーに端を発し，19 世紀のガウス，アーベル，リーマンなどきら星のように輝く巨人達によって花開きました．そこには数多くの美しい理論が生まれ育っています．みなさんが高等学校・大学初年時に学ぶ数学のほとんどはこの時代に由来します．ある本はみなさんの学んでいる数学が，いかに豊かで深い理論に関わっているかを教えてくれるでしょう．

では一体「現代数学」とはどんなものなのでしょう？ 20 世紀になって，前世紀からの豊かな理論は一層の発展を遂げ，以前とは大

きく異なる姿を見せるようになりました．様々の道具としての新しい概念や理論が提唱され，「抽象化」「一般化」され，それによって未解決の問題が次々に解かれていったのです．ある本はこうした数学の新たな展開について語ってくれるでしょう．

もう一つ今世紀の数学の大事なところは，数学の言葉が提唱され，数学が体系化されたことです．ヒルベルトからブルバキへの流れです．今はその言葉が普通に使われているため，かえって気がつかないのかも知れません．でもある本は「数学は一つだ」と主張して，このような言葉の大切さを思い起こさせてくれるでしょう．

また数学は物理学など他の学問と深い関わりを持っています．「自然は幾何学の言葉で書かれている」というのはガリレイの有名な言葉です．微分積分学はニュートン力学の誕生とともに確立されました．身近な様々の事柄の中に，実は深い数学が潜んでいるのです．ある本はこのような宝探しのガイドをしてくれるでしょう．

一方で数学は「あそび」です．ゲームや折り紙など，さまざまの頭の体操は数学を基にしています．それを追求していくと，その遊びの本質が実は深い理論につながっていることが分かるのです．ある本はこうして遊びながら数学を学ぶ方法を伝授してくれるでしょう．

こんなにいろいろの数学の世界がみなさんを待っています．
さあ数学を始めましょう！　みなさんはどの道を選びますか？

編集委員一同

はじめよう数学

④

数論の3つの真珠

数と数学，それを学ぶこと (訳者まえがきに代えて)

数の世界と数学の本

「数学は科学の女王であり，数論は数学の女王である」と 19 世紀のドイツの数学者ガウスは言いました．そして，数論の真珠と称えられた平方剰余の相互法則を発見しました．ガウスはあらゆる分野の数学ばかりではなく，地理学，天文学，物理学にも大きな貢献をした人です．磁気の強さにガウスという単位があるほどです．それでもガウスは，数論にもっとも高い価値をおいています．

数は，特に $1, 2, 3, 4, 5, \cdots$ と数えていける数は，身近で親しみやすく，とても役に立つ対象（もの）です．あなたの 1 日を考えてみても，息をするほどに不可避で，絶えず出会い，常に扱っている対象です．朝起きて時計を見る．数と出会います．体重計に乗ってみる．数と出会います．体がだるく，体温を計る．数と出会います．出かけに昼食代をもらう．数と出会います．金，長さ，面積，体積，重さ，時間，日付，温度，密度，湿度，… ありとあらゆるものが数を使って表わされます．

それは他人にも伝達することができます．伝言ゲームで文章を伝えていくと，言葉が次々と変わっていき，原形を留めないものになっていきます．しかし，数を使って表わされたことは，それほど変わってしまうことはありません．違う言葉を使う人でも，時代を隔てた人の間でも，数で表わしたものは伝わります．

洪水が起きた．寒波が来た．ペストが流行った．そういう伝説の大災厄も，水位が 25m 上がり，気温が零下 40 度に下がり，10000 人の人が死んだという 1 つのデータのほうがより多くのことを語ってくれます．印象だけで語る言葉より再現性があるのです．

単純だから役に立つ．しかし，単純に見える数の世界には，複雑で華麗な構造が潜んでいます．調べても調べても尽きることのない謎があるのです．

体系的な哲学や科学が生まれた古代ギリシャでも，数は重要な役割を果たしました．数を使って，世界と世界の調和を，理性的に理解し説明しようとした人が，紀元前 6 世紀に活躍したピュタゴラスです．小さな整数の分母分子をもつ分数を使って，美しい音色の弦楽器を作ることができるように，単純な数の比が世界の構成原理を表わすはずだというのです．そうした理想の世界観に触れたプラトンが，現実世界を理想 (イデア) の世界の投影だと考え，西洋の哲学，科学の基となる姿勢を作り上げたのです．数は弦の長さであり，数の科学が幾何学だった時代で，幾何学を知らないものは倶(とも)に語るに足らないと，プラトンは言っています．

数のいろいろな性質に，人生や生活を結びつけることが好まれました．数秘術という，錬金術や占星術と結びついていくものも生まれました．当時の生活観や世界観をより堅実なものにするために，人が「数」に仮託したものなのです．しかし，数学的に意味のある数も見つけられています．素数，双子素数，完全数，友愛数，三角数，合同数，… ．そのすべてが古代ギリシャの時代に見つけられ，今日になっても親しまれ研究され続けています．

数に関する問題の多くは，その意味だけなら誰にもわかります．たとえば，本文の中で，ヒンチンが繰り返し話題にしているのは，自然数を何かの性質をもつ数のいくつかの和で表わすという問題です．

1640 年にフェルマーは，任意の自然数を 3 つ以下の三角数の和で書くことができ，4 つ以下の四角数の和で書くことができ，一般に n 個以下の n 角数の和で書くことができると言っています．また 1770 年にウェアリングは，任意の自然数は 4 つ以下の平方数の和で書くことができ，9 つ以下の立方数の和で書くことができ，19 個以下の 4 乗数の和で書くことができると言いました．戻って 1742 年にゴールドバッハは，オイラーに宛てた手紙の中で，任意の (6 以上の) 整数は 3 つ以下の素数の和で書くことができると言っています．オイラーはその返事の中で，すべての (4 以上の) 偶数は 2 つの素数の和で書くことができるということと同値であることを注意しています (解説第 3 章 §11 参照)．

証明されているものもいないものもあり，証明されていても初等的な証明があるものもあればないものもあります．初等的でも込み入った証明しかないものもあれば，簡単な証明があるものもあります．初等的という言葉に厳密な定義はなく，高度な理論は使わないというような意味ですが，生まれてからほぼ 3 世紀しか経っていない「微積分学」を使わないことだと本書では思っておいてかまいません．しかし，本文のテーマである事実はそれ自体初等的な言葉で述べることができるので，初等的な手段だけで証明したいと思うのも，また自然な欲求なのです．

ポール・エルデシュが「ザ・ブック (天書) に書かれている証明」と言うように，どんな定理にも，その定理本来の見通しの良い単純な証明があるのかもしれません．それが証明の理想ならば，いまだ，すべての証明が得られているわけではありません．

しかし，本文の中でヒンチンが言っているように,「初等的であることが簡単であることを意味するわけではない」し,「まったく初等的な構成であっても時にどれほど複雑になり得るか」分からないこともあるのです．ヒンチンは本文で,「まったく初等的で」，しかも非常に「複雑」な構成の例を，3 つの真珠とよんで，私たちに残してくれています．

いわば，本文は数論の 3 つの真珠がしまってある宝石箱なのです．真珠の美しさを鑑賞するには，まず箱を開けないといけません．しかし今，その蓋(ふた)を開けるのにはかなりの力とコツがいるようです．けっして蓋の蝶番(ちょうつがい)が錆(さび)ついたわけではありません．宝石箱のできた時代から 50 年以上も経って，人々が宝の存在を忘れ，箱の開け方を忘れただけなのです．

本文で述べられている 3 つの定理には，ヒンチンが与えている証明より本質的にやさしい，初等的な証明は，20 世紀が終ろうとする今になっても見つかっていません．50 年以上も前にヒンチンがとり出してみせた数論の 3 つの真珠は，忘れられて，深海に眠っていたのです．その素晴らしい輝きの記憶が，何人かの人の心の底からよび覚まされ，訳者に深海に潜るようにという依頼があったのです．潜ってとり出して，そして磨いて展示するのが訳者の仕事でし

た．しかし，ダイヤモンドでならカットが古いというように，使われている言葉は古く，議論の進め方も今の読者には馴染まないかも知れません．それでも，これらの真珠は他のものに更えられない貴重なものです．

何度も何度も読んでください．きっとそのうちに分かります．何度も何度も磨いて，真珠に輝きを取り戻してください．真珠は，磨くことを知っている読者の心の中に輝くものなのです．

数学を学ぶのは確かに苦しい作業だという面があります．ヒンチンが本文で言っているように,「… の初等的解法も，簡単どころではなく，理解し習得するにはかなりの努力が必要となる」でしょうし,「できるだけ簡単になるように説明するつもり」ではいても,「数学においては (もちろん他のあらゆる科学においても)，本当に価値があり意味のあることを会得するには，どんなことにも，厳しい努力が必要とされる」ことは「覚えておいてもらわないといけない」ということです．

ヒンチンの与えている「証明は，初等的な点で素晴らしいものですが，… 」「完全に理解し会得するのには，手に紙と鉛筆をもって 2-3 週間も頑張」らないとできないほどで，でも,「このような種類の困難を克服することによって，数学」する人は「だんだんと成長していく」ものなのです．

古代ギリシャの時代は数学と音楽は同じものでした．だから，数学は音楽と同じように数楽であってもよいのです．なのに，なぜ片方が「学」になり片方が「楽」になったのでしょうか．じつはそうではないのです．ヨーロッパ諸語ではそんな区別はありません．日本語にその区別があるだけなのです．

苦しい音楽もあるように，楽しい数学もあります．ピアノやヴァイオリンのレッスンは数学を学ぶよりずっと苦しそうです．それでも，音楽の習得が困難なことは誰も非難しません．なぜ，数学は (難しいと言って) 非難されるのでしょうか．

そうです，音楽は習得できなくても別に困りません．できた方がいいけれど，できなくても困りません．しかし，数学が習得できないと困るのです．だから，文明国の初等教育では，どこでも応用数

学の基礎 (算数) が当然のように若者に強要されています．しかし，豊かになってしまった社会の住人は，強要されること自体を嫌悪します．強要されるから，数学を嫌い始める．努力せずにはなし得ない数学の習得に，届かぬ葡萄を酸っぱいと断じるキツネのように，数学は不用なものだと断じるのでしょう．そして，盛国の没落が始まるのです．

文明は数学の上に建っています．古代中国の帝王堯の優れた治世が大衆に統治を感じさせなかったように，数学は声高に功績を主張せず黙って文明を支えています．

嫌われてはいてもこれまでは，基礎的な教育における数学の地位は揺らぐこともなかったのですが，直接的には政治が，本質的には変わっていく社会自身が，その状況を変えてきています．教育における数学の立場に翳りが生まれてきています．そうした中，数学の有効性，美しさ，厳しさ，楽しさを知る僕たち数学者には，数学を護り，数学によって支えられている文明を護る義務があります．数学者もまたそうでない人も，数学の大切さや楽しさを伝えようという本を書いていて，目録の上では，あらゆる種類の，と言って良いほど数学の本があります．

数学者のための数学の本，未来の数学者に基礎知識を与える数学の本はたくさんあります．大学の基礎教育としての数学の本なら，教科書，参考書，演習書，それも難しいものからやさしいもの，理論的なものから実践的なもの，歴史的な観点から概念・技術のルーツを語るものまで多量にあります．ちゃんと読むと，結構面白いのですが，これも強制されると面白くなくなるのでしょう．小学校から高校までは，検定教科書があり (昔の教科書は結構面白かったものですが)，参考書があり，問題集があります．数学の雑誌もあるし，受験数学の雑誌もあり，数学・算数の教え方についての雑誌もいくつかあります．新書や文庫にも読ませる工夫に溢れた本が出ています．

どれも，読めば面白く，教科書でさえ，感心するような工夫がされたものも少なくありません．

それでいて，本屋に行ってみても，あまりちゃんとした数学の本がおかれてないことが多いのは，どうしてなのでしょう．何故か数学の本は敬遠されています．

数学の本といっても，あまり抵抗感なく誰にも受入れられているものもあるようです．たとえば，数字の絵本，数学 (算数) パズルの本，…．要するに，算数・数学が嫌いでない (年代の) 子供を対象とする本なのだということでしょうか．

しかし，専門知識をもたない普通の大人が楽しみながら，そして時には苦しんででも読みたいと思う本が少ないのです．江戸川乱歩が描く名探偵・明智小五郎は，仕事のない夜は，徒然に，高等数学の問題を解いて過ごしていました．

推理小説が流行っています．でも，殺人の技術を習得するために読むわけではありません．数学だってそんな風に思って読めば，面白いのにと思います．読まないから分からないだけで，読めばきっと面白い．

それでも，読んで分かれば面白いくらいの主張にしておかないと，ここまで読んだ読者に数学至上主義者の本かと放り投げられてしまうかもしれません．といって僕が数学至上主義者でないわけではありませんが．

推理小説にもいろんなジャンルがあります．いまや推理小説は探偵小説，警察小説，犯罪小説，サスペンス，ホラーを含んで膨張し，エンターテインメント小説だと言ってもよく，童話や昔話から進化してきたファンタジーや SF とも融合してしまっています．古き良き時代の推理小説には，ペダンティズムが薫ります．どれも面白い．数学の本にもそんなヴァラエティがあってもいいし，音楽のようにいろいろな楽しみ方があってもいいはずです．

あなたには，数学を単に固定した教科として見るのではなく，人類の遺産・文化としての数学，文明を支える基盤としての数学を学んで欲しいと思います．上に述べたようにいろんな種類の数学の本があります．自分で，自分の世界観を作るために数学に関した本を読み，自分を高めてください．本書もきっと，そのための役に立つと思います．

本書の成り立ち

さて，本書はどんな本なのでしょうか．

本文の著者は，旧ソ連の数学者でアレキサンドル・ヤーコヴレヴィッチ・ヒンチン (Александр Яковлевич Хинчин) という人です．1894 年 7 月 19 日にロシアのカルージュスカヤ・グベルニヤ，コンドゥロヴォで生まれ，1959 年 11 月 18 日にソビエト連邦のモスクワで亡くなりました．彼が書いたロシア語の Три Жемчужины Теории Чисел 第 3 版 (1979) という本[1]を，日本語に訳したものが本書の中心部分です．このタイトルは，直訳しても「数論の 3 つの真珠」となって，非常に魅力的なものです．英訳のタイトルも素直に “Three Pearls in Number Theory” となっています．初版は 1945 年です．所々(特に第 3 章では) 記号や書き方を平易にしようとした校訂が，A.B. シドロフスキー (本文の初めに出てくる編集者) によってなされていますが，内容は第 2 版 (1946) と大きく変わっていません．じつは，原著第 2 版のドイツ語訳からの重訳が，1957 年に木下素夫訳でみすず書房から出版されていました．それも絶版になって久しく，存在すら忘れられようとしています．

半世紀以上も前に書かれたこの本を，なぜいまロシア語から訳し直すのでしょうか．時代を越えた素晴らしい数学と，数学に対する著者の姿勢，良い数学者を養成することへの静かだが強い著者の情熱．ある意味で，失われていく古き良き時代の数学の世界の雰囲気を，もう一度現代のものとして蘇らせたい．そういう熱い情熱で数学を語る人がいたことを，思い出としてでなく，今必要なことなのだとすべての人が想うべきときではないでしょうか．

ヒンチンが本文を書いた頃のソヴィエト連邦では，ナチス・ドイツとの戦争で，ヨーロッパ・ロシアの国土の多くが荒廃していました．人口の多さと国土の広さだけが財産とも言えるほど疲弊していたのです．ソヴィエト連邦も成立したばかりで国力を培うことが急務でした．ソヴィエト連邦にとって，科学こそが正しく国を富ませる原動力であると信じられており，そのために科学知識の普及が重要視され，特に基礎科学の担い手の育成に力が入れられていました．

---

[1] この本の表紙が本書の p.78 にある．

帝政ロシア時代の，農奴も存在するような前近代的な体制が打倒された後に興った，ロシアでは初めての民主的政治形態だったのです．心ある科学者は，国のため，そして世界のため，人類のためと信じて教育に力を注いでいたのです．

ヒンチンもまた多くの教科書を，というより若い数学者を養成する目的の書物を書いています[2]．本文にも，優れた若い才能を育てようという，彼の熱意が横溢(おういつ)しています．そのため，彼の語り口は，優しいものとは言えません．

しかし，ヒンチンが見せてくれる 3 つの真珠は，それぞれ素晴らしいものです．今このような話題を探そうとしてもなかなか見つかりません．第 1 章でさえ，初等的ではあっても，非常に複雑な構成をもっています．そして，第 2 章は第 1 章の倍，第 3 章は第 2 章の倍の長さになっています．どれも，しばらく数学界で懸案になっていた問題で，当時若かった数学者が解決を与えたものです．柔軟な頭脳と体力がなければ解けなかっただろうと思われる問題です．それをヒンチンが整理したものが本文の 3 つの章なのです．

前にも触れたように証明はすべて「初等的」なのですが，そのためにむしろ構成は複雑になっていきます．構成が複雑になっていくと，証明の途中で何をしているのかわからなくなって，富士山麓の樹海に迷いこんだような気がしてくるでしょう．特に第 3 章は足元に光の射さない深い森にいるような感じがするときもあるでしょう．整理された証明を読むだけでもそうなのです．最初に証明するときは，どの方向に正しい道があるのかまったくわかりません．発見者は非常に強い意思の力をもっていたのでしょう．

今，大学に入学してくる学生に講義をしていて残念に感じることは，やさしいことであっても，少し複雑になると，それをやり通す力がないということです．むしろ，やり通す意思の力がないとい

[2]ヒンチンの著書の多くは日本語に訳されている．『数論』(銀林浩，麻嶋格次郎訳，商工出版,1958),『確率論入門』(グネジェンコとの共著，渋谷政昭，渡辺毅訳，みすず書房,1956),『待合せ理論入門』(修正 3 版，森村英典訳，広川書店, 1966),『統計力学の数学的基礎』(河野繁雄訳，東京図書, 1971) など多数あるが，残念ながら『数学解析 8 講』(馬場良知ほか訳，大竹出版，2000) を除いて絶版である．

うことです．すぐに答えを欲しがって，すぐにわからないことはわかろうとしていないと感じることがあります．わからないことを，いわば謎を謎のままで体の中に抱えておくことは，とても大切なことなのですが．それが多分，とても気持ち悪く思うのでしょう．誰だってわからないことをわからないままにしておくことは気持ちの良くないことです．しかし，そうしていれば，問題を意識的または無意識的に考え続け，いわば心の中で熟成して，あるとき気がつけば，解けてしまっているということがあるのです．大きな数学の発見ほど，そうして生まれることが多いのです．

誰にでもすぐにわかるような問題が詰まらないというのではありません．そういう問題の方が基本的で，しっかり把握しておくべきだという考え方もあります．また誰にも解けなかった難しい問題に対して，概念や方法を創り出し，すべての人に当り前と思えるようにすることは，数学の１つの理想でもあるのです．しかし，最初に突破するときはどんなに強引でも力づくでも解ければいいし，そうでなければ解けないことも多いのです．一旦解けてしまえば，やさしく解く方法も見つかるというものです．

今の時代にこそ，読むための数学の本でなく，自分で考えるための数学の本が必要なのではないでしょうか．高校生に向けてのこのシリーズの中に本書を選んだ編集委員の意図はそのことだったのでしょうか．

意図はわかるものの，今の高校生に提供するには，そのままではやはり難しすぎるような気がしました．できる限り訳註もつけて補足しましたが，それでも難しいと感じます．もちろん，直接に本文にアタックして読解のできる読者はそうした方がいいでしょう．その場合にも，一度や二度の挫折にはくじけないで何度も何度もアタックして欲しいと思います．山もある程度は高くなければ「貴く」ないように，本書は (予備知識は要らないのに) 難しい，ということにこそその真価があるのですから．

僕も，訳すために何度か読み返して，何とか理解はしました．素晴らしいと思いました．しかし，何か物足りません．本文には，さらっと触れられているだけのテーマや定理がいくつかあります．と

ても面白そうです．でも時代が移って，解決されているかも知れません．どうなっているのだろうか？　じつに落ち着かない気持ちになりました．僕はこの分野においてはアマチュアなので，素朴な好奇心が掻き立てられたのです．それで，調べてみました．しかし，調べ方が悪いのか，日本語で出版されている本では，十分この好奇心を満足させられませんでした．本文を苦労して読んだ読者なら，きっと同じ思いに駆られるでしょう．そうだとするなら，今までに分かっていることを調べるのも僕の義務のような気がしてきたのです．

書いていくうち興味が広がり，どこで止めるかの方が問題になってきました．できあがったものは結局，自分が読みたいものになりました．内容的には本文の内容を含んだ『加法的整数論入門』というようなものです．本文そのものの解説というより，本文の内容とその後の進展の解説です．

しかし，そのため，記述に難易度や視野の広がりに凸凹ができてしまいました．普通の数学の本のつもりでいると，違和感があるかも知れません．たとえば，解説の第 1 章 §2 の数学的帰納法は，フェルマーの無限降下法を説明するためにだけ書き始めたのですが，多少趣味が過ぎたようでもあります．それでも，きっと楽しんでいただけると思っています．なにしろ，僕は楽しんで書きましたから．

解説は，高校生以上の数学を愛するすべての人が，それだけを読んでも分かるものにしたつもりです．しかし,「初等的」という制約を課したので，述べきれない部分があります．できるだけ文献を挙げておきましたが，ほとんどが外国の数学雑誌や書籍なので，タイトルの日本語訳で内容を推測してください．いつの日か，読者の中から，原論文を読んで，そして自分自身の歩みを始められる人が生まれると嬉しいと思います．

本書の読み方

本書は，ヒンチンの本文が 3 章，訳者の解説が 3 章，作業の素材となる数表が 1 章分という構成になっています．本文をその順の通りに読破し，それからそこに触れてあるいろんな話題について，読み物を読むように解説を読んで貰うというのが，もっとも正統派の

読み方とは言えます．

しかし，多分それはもっとも困難な読み方だと思いますし，じつを言ってそのように最初から順に読んで貰うことを期待してはいません．ヒンチンの書いた本文と違って，解説の方は，大小様々な宝石が難易度の順でなく，関心の順序に並んでいる陳列箱のようなものです．

もっとも抵抗感の少ない読み方を 1 つ紹介しましょう．最初は本文の各章の導入部だけ読んでください．各章の内容は以下のようなものです．

第 1 章は，自然数をどのように 2 つに分割してもどちらかのクラスには好きなだけの長さの等差数列が含まれる，というバウデットの予想が話題になっていた歴史から始まります．最初に証明したファン・デル・ヴェルデンは，予想をそのままの形でなく，もっと一般な形の定理に昇華させて証明したのです．第 1 章の内容は，彼の証明を若干簡易化したルコムスカヤの証明を紹介したものです．

第 2 章では，自然数の部分集合に密度を定義します．その簡単な性質からでも整数の面白い事実を示すことができます．さらに，2 つの集合の和として得られる集合 (和集合ではありません) の密度と元の集合の密度との関係についてのシュニレルマン予想がマンによって証明されました．その証明をアルティンとシェルクが簡易化したものが紹介されています．

第 3 章は，ウェアリングの問題です．問題の肯定的解決は 1907 年にヒルベルトによってもたらされましたが，見通しも悪く初等的でもない証明でした．それだけ独創的だったということです．10 年ほど後にハーディー–リトルウッドとヴィノグラードフが明快なアイデアで新しい証明を与えましたが，それも微積分を駆使したものでした．そして 1942 年になってやっとソ連のリニクが初等的な証明を与えたのです．

これくらいのことが分かったら，解説をざっと眺めてください．解説は初めから順に読む必要はありません．もちろん，順に読んでも良いように書いてありますが．パラパラッと見て，気に入ったところとか分かりそうなところから取り掛かってください．その箇所

に必要なことがそれ以前に書いてあると指示してあれば，その部分を眺めてください．

「眺める」という言葉が気になりますか？　眺めるというのは字面を眺めるという気分で，単に文字を読むというか，意味が分かってもわからなくても良いから，読み下すということです．数学の本を「読む」というのは，理解しながら読むということです．

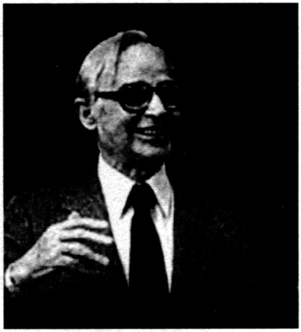
解説では，高校生が本格的な数学の本を読むときに感じるであろう障害について，少しくどいくらいに雑談風のコメントをつけてみました．ぱらぱらと眺めているうちにきっと何ヶ所か読めるようになるでしょう．

そこで自信がついたら，本文にアタックしてみてください．一度には１つの章だけで構いません．草臥(くたび)れたら，本書のことはしばらく忘れても構いません．でも，きっともう一度手に取りたくなる時がきます．あなたにとっても，それだけの魅力を秘めた本であることを僕は信じています．

解説の附録の数表は本当の附録です．理論的な記述に疲れたとき，それでも数の世界で遊んでほしい．そのための (素材としての) ブロックのようなものです．説明があって，問題があって，解ければいいというような本だけが数学の本ではないことを知って欲しくて付けてみました．何かの理論や事実を習ったら，それを具体的な数を使って確かめてみる．必要な数表を何枚かコピーして，何かの性質で色を塗ったり，印を付けたりして遊んでみてください．けっして，本自体に色を塗らないでください．そうでないと，別の遊びをするときの邪魔になってしまします．

人名索引には，基本的には本書の中に出てくるすべての人の，生没地と生没年月日を含む情報を載せてあります．数学は人の行う営みであることを知って貰いたいのです．昔の人になると諸説紛々のことも多いようです．そんな場合にはあまりこだわらず，信用できそうな説を挙げてあります．細かい点では違っていることがあるかもしれません．

本書用のホームページ (http://www.com.mie-u.ac.jp/~kanie/tosm/pearl/) を僕が運営しているホームページの中におき，ミス



ファン・デル・ヴェルデン

プリントなどの情報を載せます．間違いを見つけた読者は，ぜひそこにあるアドレスにメールしてください．また，人名索引は，他の僕の著訳書に登場する人物と合わせたものを作っていますので，ご利用ください．

原著では，第 1 章 §1 - §6，第 2 章 §1 - §4，第 3 章 §1 には節のタイトルがついていませんが，読みやすさを考えて，タイトルをつけました．

ファン・デル・ヴェルデンの思い出

最後に，第 1 章の定理を最初に証明したファン・デル・ヴェルデンの思い出話を少しだけ紹介しておきましょう．「1926 年のある日，エミール・アルティン，オットー・シュライヤーと昼食を取りながら，彼らにオランダの数学者バウデットの予想について話した．」と彼の話は始まります．アムステルダム生まれでアムステルダムとゲッティンゲンの 2 つの大学で学んだオランダ人の彼は，当時ハンブルグに来ていたのです．

「昼食の後，我々はハンブルグ大学数学教室のアルティンの研究室に行き，証明を見つけてみることにした．黒板の上にいくつかの図式を描いた．」議論の中で彼らには閃きに似た思いつきが幾度も訪れ，そのたびに議論が新しい局面を迎え，アイデアの 1 つが最後には解決へと導いたというのです．

アイデアの一番大きな点は，バウデットの予想をより一般的で強



アルティン

い命題におき換えることでした．帰納法を使える形にし，しかも定理を数列に対してだけでなく数のブロックの列に対しても使える形にします．アルティンとシュライヤーもいくつかのアイデアを出したそうです．帰納法で示すとして，いつも気になるのは，自明な最初の段階ではなく，その次の最初に自明でない値での証明です．ファン・デル・ヴェルデンはその部分はこれ以前に示してあったようで，それを二人に説明し，一般の場合にも成り立つという確信を得たそうです．しかし，アルティンたちはそれには納得できず，帰納法のもう１つ次の段階も確かめたいと言ったので，彼はその場合の証明をしたのだそうです．

そこで，ファン・デル・ヴェルデンの有名なたとえ話が述べられます．

「それは木からリンゴを摘むことに似ている．ある人があるリンゴを取り，別のリンゴがもう少し高い所になっていれば，もうちょっとした努力でもう１つリンゴを取ることができることがわかるということも起こるかも知れない．私の隣に立っている人は私が最初のリンゴを得たことしか見ていないので，私がもう１つのリンゴを取ることができるかどうか疑わしく感じるだろうが，私自身は単にリンゴを取るだけでなく，リンゴの摘み方を体感したことにもなる.」

少しわかりにくいですね．アルティンとシュライヤーはアイデアは出したが実際に証明を考えたわけではなく，ファン・デル・ヴェルデンが示した証明だけしか見ていないのです．ところがファン・

デル・ヴェルデンは自分でその証明を考え出したので，状況が少し変わったときにもどのようなことが起こるかが予測できた，ということなのでしょう．

人が 1 つのリンゴを取っているのを離れた場所から眺めていても，それ以外にリンゴがあるかどうかは分からないが，リンゴの木の下でリンゴを見ながらリンゴを取っている人にはほかにもリンゴが生っているのが分かるという喩えなのです．

だから教科書に書いてある定理の証明を読んで理解しただけでは先に進むことは難しく，何か新しいことをしようというなら，その定理の証明を自分で考えてみるほうが良いという教訓です．といって，すべての定理をそうするわけにもいかず，自分の (生涯の持ち) 時間との兼ね合いで選択するということになるのでしょう．その選択のウェイトのかけ方がその人の数学のスタイルを決めていくことになるのです．

謝辞

解説を書くために，主に [エリッソン (1971)]， [ガウス (1801)]，[ゴールドマン (1998)]， [ディクソン (1919-23)]， [ナゲル (1964)]，[ハーディー，ライト (1979)]， [ベイカー (1984)]， [リーベンボイム (1991)]， [ローズ (1994)] を参考にしました．

鳥羽商船の佐波学氏には，原稿を通読して，ときに暴走しがちな僕の頭を冷やしてくれたり，ミスプリントを見つけてくれたり，その有益なコメントに感謝します．

また，編集者に深く感謝しています．本文の翻訳は 1 年以上も前に終わっていたのにもかかわらず，訳者のわがままで，解説部分がどんどん膨らんで行き，その目処がついたと思ったら，別の導入部を作りたいなど，本書がどのような形になって行くのかわからない状態が続きました．不安も不満も胸に納め，じっと待っていてくれたことに，本当に深く感謝しています．

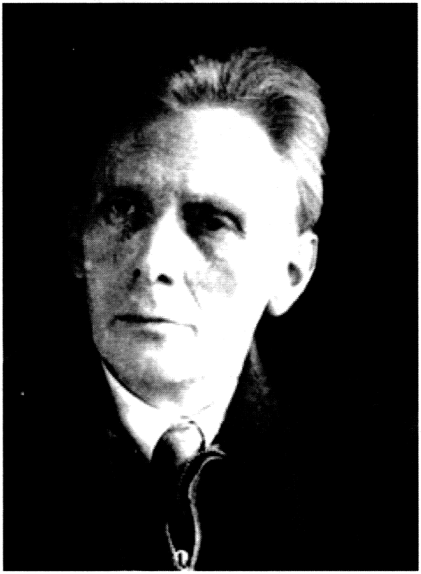
2000 年 4 月

蟹江幸博

ТРИ ЖЕМЧУЖИНЫ ТЕОРИИ ЧИСЕЛ

数論の3つの真珠

ア・ヤ・ヒンチン



ア・ヤ・ヒンチン

編集者まえがき

この薄い本は今から 30 年以上も前に書かれました．しかしその内容は広い読者層にとって — 現在の数学の愛好者にとっても，その価値を保ちつづけてきました．2 つの版が，1947 年と 1948 年に出版されています．このため今では手に入れにくいものになり，この第 3 版の出版が待ち望まれていたのです．

著者である高名な学者－数学者であり傑出した教育家でもある－アレキサンドル・ヤーコブレヴィッチ・ヒンチン (1894-1959) は，ソビエト連邦科学アカデミーの通信会員であり，モスクワ大学の講座主任でした．本書の内容は 3 つの有名な数論の問題に捧げられています．それは大変単純に定式化されますが，難しく，そして多くの大数学者たちの努力にも屈せず，それにもかかわらずもっとも初等的な方法で解かれた問題なのです．アレキサンドル・ヤーコブレヴィッチ自身，数論では最高級の専門家で，その発展に大きく貢献をしています．この科学の問題と方法を深く理解している彼は，驚くほどの熟練と優美さを見せて，問題とする定理の証明を説明しています．そのため，この長い時の流れの間も，当然のことですが，私たちのこの国の，また本書の翻訳が出版された国々の，数学を愛する人々の間で，人気を博してきたのです．確信をもって言うことができますが,「数論の 3 つの真珠」は，多くの若い数学者たちを数論の問題に取り組むように仕向けることによって，この科学の発展に大きな役割を果たしてきました．

本書で問題となっている 3 つの定理はすべて，当時は若く新人の数学者で，後には有名な大数学者になった人々の手で，初等的な方法で解かれました．

自然数の集合を分割した部分集合における等差数列に関する定理を証明したオランダ人の B.L. ファン・デル・ヴェルデンは，広く知られた数学者かつ数学史家になりました．彼の代数学の著書は，

この 40 年間数学者必携の書物になっています．

加える数列の密度による数列の和の密度の評価に関する定理－加法的整数論で大きな役割を果たしている－を証明したアメリカ人 H.B. マンは，数学で多くの他の重要な結果を得ています．

自然数を自然数のベキの和で表わすという有名なウェアリングの問題に初めて初等的な解法を与えた，我々の同国人である Yu.V. リニクは，もっとも重要なソビエトアカデミー会員になり，数学と数論の発展に多くの新しいものをもたらしました．1972 年の早すぎる彼の死去は，大きな損失でした．

ア・ヤ・ヒンチンは，戦争によって学校の長椅子や大学の講義室での好きなことから引き離され，また戦後，異常な程の熱意で数学の基礎の習得に加わった，数学に興味を持っていた 1940 年代のソビエトの若者に，その著書を捧げたのです．このことについては，本書のまえがきの代わりに書かれた前線への手紙が物語っています．そして本書の記述も前線への手紙の形で行われています．その英雄的な時代に敬意を表わして，著者のテキストをそのままの形に出版することになりました．編集校閲にあたっては，些細な文体上の修正をするに留めることにしました．

ヒンチンの著書のこの再版が広い範囲の数学愛好者に好意を持って受け入れられ，本書の中でこんなにも鮮やかに物語られる「数論の 3 つの真珠」が，これまで通り，もっとも古い科学である数論の魅惑的な問題によって，多くの人々をその深い学習へ駆り立てることを，出版局は期待しています．

1978 年 7 月 10 日　　A. シドロフスキー

戦線への手紙

(序に代えて)[1]

親愛なるセリョージャへ[2]

病院から送られた貴方の手紙は三重にも私を喜ばせてくれました．何よりもまず,「なにかある数学の小粒の真珠」を送って欲しいという依頼から，貴方が実際に快方に向かっており，単に勇敢な戦士として，友人たちを安心させようとしているのではないと分かったことです．これが1つ目の喜びでした．

さらに，この戦争では，貴方のような極めて若い戦士たちが，戦争まではその身を捧げ，戦争によって引き離された自分たちの大好きな活動に，わずかな暇を見つけては熱心に取り組んでいる，というようなことを私に考えさせてくれました．先の世界大戦ではこういうことはありませんでした．当時戦線に送られた若者は，自分の人生が折りとられ，以前には人生を満たしていたものが起こりようもないおとぎ話になってしまったと，たえず感じていたものでした．それが今日では，戦争の合間に学位論文を書きあげ，短い休暇で帰るときに論文審査を受ける人さえいるのです！　これは貴方たちが，戦争での働きと愛する仕事 — 科学，芸術，実践活動 — が，同じ1つの大義の2つの輪であると，心の底から感じているからではないでしょうか？　もしもそうなら，そう感じていることは，銃後にある私たちがここでこんなにも熱狂している貴方たちの勝利の主要

---

[1] ［訳註］末尾の日付けを見てもわかる通り，第2次大戦中のヨーロッパ戦線にいる教え子への手紙という形を取っている．

[2] ［訳註］セリョージャとはセルゲイという男性の名前の指小形で，自分より年少の知人や家族，親しい間柄を示すときに使われるものである．しかし，以下の本文での相手に対して使っている人称代名詞を見ても，本文中に述べているように個人的な付き合いはないということかも知れない．実際に対応する個人が存在したのか，本書を書くためだけの設定なのか，今は分からない．

な原動力の１つなのではないでしょうか？　この考えはとても私を喜ばせてくれました．これが２つ目の喜びでした．

そこで，どんなものを貴方に送ろうかと考え始めました．貴方を非常に親しく知っているわけではありません．私の講義に出席してくれたのも１年だけです．それでも，科学に対する貴方の深く真面目な態度は私の心に強く残っていましたので，見てくれは良くても科学的な内容の乏しい「玩具のようなもの」を貴方に送りたくはありませんでした．一方で，貴方の素養があまり深いものでないことも分かっていました．大学の椅子で過ごしたのも１年間のことですし，３年もの間絶えず前線にいたのでは勉強する暇だってなかったでしょうし．何日かよく考えて，１つの選択をしました．それで良かったでしょうか — どうか貴方がそれを判断してください．私としては，貴方に書き送るこの３つの算術の定理は，我々の科学の本物の真珠であると考えています．

算術，このもっとも古くそして永遠に若い数学の分野では，ときおり素晴らしくまた一風変わった問題が現れることがあります．その内容は初等的で，中学生にも[3]理解できるほどのものです．問題は普通，数の世界を支配するある非常に簡単な法則を証明することです．その法則は特別な場合に調べてみるといつも成り立っているのですが，実際常に成り立つことを証明しなければならないというわけです．問題の見かけの簡単さにも関わらず，それを解くのに何年も，時には何世紀にもわたって，その時代の大学者たちの努力が必要なことがあるのです．とても面白いことだと，思いませんか．

貴方のためにそのような問題を３つ選んでみました．それらはすべてつい最近解かれたもので，その来歴には２つの際だった共通の特徴があります．第１に，この３つの問題はどれももっとも初等的な算術的方法で解かれたことです (初等的であることと簡単であることを混同してはいけません．読めば分かりますが，どの問題の解答もあまり簡単ではなく，それをよく理解し習得するには，少なか

---

[3] ［訳註］ここでは中学生と訳したが，ロシアの初等教育の制度では小学校と中学校を一緒にした初等学校があって，それに所属する生徒という意味の言葉が使われている．証明は分からなくとも数学的な内容＝意味は分かるだろうということだろうか．

らず努力しなければならないでしょう)．第2に，この3つの問題は,「長老」級の学者が何度も解決に失敗したあとで，非常に若い，そう貴方と同じ年頃の新進の数学者によって解かれたことです．これはまったく，貴方のような新進の学者にとって，未来に希望を抱かせる刺激的な話だし，科学的な挑戦への誘いとしても素晴らしいものです．

これらの定理を述べるための仕事をすると，その壮麗な証明の構造の中に深く分け入ることになりましたが，それは大きな喜びを与えてくれました．

これが3つ目の喜びでした．

貴方のさらなる成功を祈ります．戦いにおいても，科学においても．

1945年3月24日　　　　　　あなたのA. ヒンチンより

第1章

等差数列に関するファン・デル・ヴェルデンの定理

§1　1928年ゲッティンゲンの夏

1928年の夏，私はゲッティンゲンで何週間かを過ごしました．いつものように，夏学期[1]にかなり多くの外国の学者が集まってきていました．そのうちの多くの人とは知り合いになり，幾人かとは友達にもなりました．私が着いた頃に，集まっていた数学者たちの間で大きな話題になっていたのは，オランダ人の若いファン・デル・ヴェルデンの感銘を与える結果[2]でした．彼も今では有名な学者ですが，当時はまだ新進の青年でした．この結果は，ここゲッティンゲンで得られたばかり，それも私が到着するほんの数週間前のことだったのです．私が出会ったほとんどの数学者はこのことを興奮して話してくれたものです．

この問題の由来は次のようなものです．この地のある数学者が (名前を忘れてしまいましたが[3])，研究中に次のような問題にぶつかったのです．自

[1] ［訳註］夏学期といっても，夏に学期があるわけではない．特にヨーロッパでは大学の夏休みが長く，その期間を利用して，外国の大学や研究所に出掛けていき，研究上の交流をする習慣がある．学生がいなくなった寮などに泊まることができ，人気のある大学では，三々五々来往する人々で学者村のような観を呈することがある．

[2] ［訳註］ファン・デル・ヴェルデン (1927)『バウデット予想の証明』に以下の内容が証明されている．また，発見のいきさつがファン・デル・ヴェルデン (1965)『バウデット予想の証明はいかにして発見されたか』に詳しく述べられていて，以下ヒンチンが述べていることには伝聞ゆえの誤解が多少あるようだが，問題にするようなことはない．

[3] ［訳註］ヒンチンが名前を忘れたと言っているのは上の註で触れたバウデットのことである．

然数全体の集合が，どんなふうにでもよいから，2 つの部分に分けられたとしなさい (たとえば，奇数と偶数とか，素数と合成数とか，また他のどんな仕方でも良いから)．そのとき，この 2 つの部分の少なくとも一方には，任意の長さの等差数列が含まれることを示すことができるだろうか？(ここで，またこれ以降も，等差数列の長さというのは単に項の数のこととします．) この質問を受けた人はみな，問題は一見非常に単純なものだと思いましたし，答えが肯定的だというのもほとんど当り前のことのように見えたのです．しかし，解こうと試みても，最初のうちは何も得られませんでした．でも，ゲッティンゲンの数学者と外国からの訪問者はいつも互いに協力しあう伝統があったので，なかなか解けようとしないこの問題はすぐに皆の興味の的になったのです．長老の学者からほんの学生まで，あらゆる人が取り上げたものでした．張り詰めた努力が数週間続き，ついに問題はゲッティンゲンに留学に来たばかりの若いオランダ人，ファン・デル・ヴェルデンの攻撃に屈したというわけです．私は彼と親しくなり，彼自身から彼の発見した解答を聞くことができました．解答は初等的なものでしたが，けっして単純なものではありませんでした．問題は深いものであり，見た目の簡単さは見せかけのものだったのです．

つい最近になって，M.A. ルコムスカヤ (ミンスク[4]) は，彼女が最近発見した，ファン・デル・ヴェルデンの定理の新しい，ずっと簡単で見通しのよい証明を送ってきたので，以降それを貴方に書きます．彼女は快く許してくれましたので．

§2　ファン・デル・ヴェルデンの定理

実際の所，ファン・デル・ヴェルデンは要求より少し強いことを証明しました．初め彼は，自然数が 2 つの部分ではなく，任意個数 k 個のクラス (集合) に分かれていると仮定しましたが，後に，これらのクラスの少なくとも

---

[4] ［訳註］ミンスクはベラルーシ共和国の首都で，モスクワとワルシャワを結ぶ線分を 2：3 に内分した辺りに位置する．

どれか 1 つの中に，与えられた長さ l (どれほど大きくてもよい) の等差数列が存在することを保証するだけだったら，自然数全体の列[5]を分割する必要がなく，自然数のある区間[6]を取れば十分であることが分かりました．この区間の長さ $n(k,l)$ は，k と l の関数です．当然のことですが，この区間をとるとき自然数が $n(k,l)$ 個並んでいればどこにとってもよいのです．

こうして，ファン・デル・ヴェルデンの定理は次のように定式化されます．

k と l を任意の自然数とする．そのとき，ある自然数 $n(k,l)$ が存在して，自然数全体の列の長さ $n(k,l)$ の任意の区間をどんな仕方で k 個のクラスに分けたとしても (その中には空集合があってもよい[7])，このクラスのどれか 1 つには長さ l の等差数列が存在する．

明らかに，$l = 2$ のときは，この定理が正しいことは自明[8]です．そのためには $n(k,2) = k+1$ とおけばよいのです．実際，$k+1$ 個の数を k 個のクラスに分ければ少なくとも 1 つのクラスには 2 個以上の数が含まれますが[9]，任意の 2 数は長さ 2 の等差数列をなしており，定理は証明されます．数 l に関する数学的帰納法で定理を証明しましょう．以下ではある数 $l \geqq 2$ と任意の値 k に対して定理がすでに証明されているとし，そのとき数 $l+1$ (と，もちろん任意の値 k) に対しても定理が成り立つことを示しましょう．

---

5 [訳註] ここでわざわざ自然数全体の列という言い方をしているのは，自然数全体を単なる集合として考えるのでなく，順序を込めて集合を考えていることを表わしている．

6 [訳註] 区間というのは，順序集合としての自然数の中の区間という意味合いのもの．ある $a < b \in \mathbb{N}$ に対して，$[a,b] = \{n \in \mathbb{N} \mid a \leqq n \leqq b\}$ と定義されるもののこと．一々，自然数全体の列の区間と言わないで，自然数の区間という言い方をすることにする．

7 [訳註]「k 個以下のクラスに分けても」ということ．

8 [訳註] 自明というのは語感の伝えにくい言葉である．数学用語というわけでもないのだが，といって，数学以外で使えば価値観を含むようになって使うことはあまり奨められない．この場合も，明らかで自明だと言っておいて，数行の証明が書かれている．

9 [訳註] これは典型的な鳩ノ巣論法 (引き出し論法とも言う) である．証明のポイントは鳩ノ巣論法にどう持ち込むかということである．

§3　証明の方針

仮定に従えば，どんな自然数 k に対しても自然数 $n(k,l)$ が存在して，長さ $n(k,l)$ の自然数のどんな区間をどんな仕方で k 個のクラスに分けたとしても，少なくともどれか 1 つのクラスには長さ l の等差数列が存在しています．そこで私たちの問題は，どんな自然数 k に対しても $n(k,l+1)$ が存在することを証明することです．この問題を，数 $n(k,l+1)$ を具体的に構成して解くことにします．そのために

$$q_0 = 1, \quad n_0 = n(k,l)$$

とおき，数 $q_1, q_2, \cdots, n_1, n_2, \cdots$ を次のようにして次々と定めます．ある $s > 0$ に対してすでに q_{s-1} と n_{s-1} が定義されていれば

$$q_s = 2n_{s-1}q_{s-1}, \quad n_s = n(k^{q_s}, l) \quad (s = 1, 2, \cdots) \tag{1}$$

とおきます．これによって，どんな $s \geqq 0$ に対しても数 n_s, q_s が定義されます．ここで，$n(k,l+1)$ として数 q_k をとることができることを主張します．したがって，長さ q_k の自然数の区間をどのような仕方で k 個のクラスに分けたとしても，少なくとも 1 つのクラスの中に長さ $l+1$ の等差数列が存在することを証明しなければなりません．本章の残りのすべてでこのことを証明することにしましょう[10]．

簡単のために $l+1=l'$ とおくことにします．

[10] ［訳註］q_k を具体的に計算すると，急激に大きくなることがわかる．たとえば，$n(2,3) = 4 \times 3(2^6+1) = 12 \times 65 = 780$ であり，$n(3,3) = 8 \times 4(3^8+1)(3^{4\times4(3^8+1)}+1) = 32 \times 6562 \times (3^{16\times6562}+1) = 209984 \times (3^{104992}+1)$ となる．高々3 項の等差数列を得るためにこれだけの長さの区間を用意する必要があるのである．有限の長さの区間では不可能ではないかと感じた読者も，少しは安心できるかも知れない．

§4　数と区間のタイプ

さて，長さ q_k の自然数の区間 Δ をどのようにでもよいから k 個のクラスに分けたとします．この区間の **2 つの数** a, b が同じクラスに属すとき，**同じタイプ**であると言い，$a \sim b$ と書きます．区間 Δ に含まれる長さの同じ 2 つの区間 $\delta = \{a, a+1, \cdots, a+r\}$，$\delta' = \{a', a'+1, \cdots, a'+r\}$ は，$a \sim a', a+1 \sim a'+1, \cdots, a+r \sim a'+r$ を満たすとき，**同じタイプ**であると言って，$\delta \sim \delta'$ と書きます[11]．明らかに，区間 Δ の数が属する可能な異なるタイプの数は k です．$\{a, a+1\}$ の形の区間 (つまり，長さ 2 の区間) に対しては，可能なタイプの数は k^2 であり，長さ m の区間に対しては，可能なタイプの数は k^m です (当然のことですが，これらのタイプのいくつかが，実際には区間 Δ の中にはないこともあります)．

$q_k = 2n_{k-1}q_{k-1}$ だから ((1) 式参照)，区間 Δ は長さ q_{k-1} の $2n_{k-1}$ 個の区間に分けることができます．今考えたように，このような区間には $k^{q_{k-1}}$ の異なるタイプがあり得ます．しかし，区間 Δ の左半分[12]にはこのような区間が n_{k-1} 個含まれており，その上 (1) 式により $n_{k-1} = n(k^{q_{k-1}}, l)$ です．このため，数 $n(k^{q_{k-1}}, l)$ の意味から，次のことを示すことができます．区間 Δ の左半分には，長さが q_{k-1} で互いに同じタイプの l 個の区間

$$\Delta_1, \Delta_2, \cdots, \Delta_l$$

からなる等差列が含まれています．ここで，言葉の節約のために，長さの同じ区間 Δ_i が，それぞれの最初の数が等差数列をなすときに，**等差列**をなすと言っています[13]．**等差列** $\Delta_1, \Delta_2, \cdots, \Delta_l$ **の公差** d_1 とよぶのは，この列

[11] ［訳註］区間の普通の表わし方では $\delta = [a, a+r]$，$\delta' = [a', a'+r]$ と書くものだが，この章の中では区間の中の各元を意識したいので，あえてこういうように区間に属するすべての自然数をあげた形で表わしている．

[12] ［訳註］Δ の長さは $q_k = 2n_{k-1}q_{k-1}$ で，左半分の区間の長さは $n_{k-1}q_{k-1}$ である．

[13] ［訳註］ここで，帰納法の仮定を使うために，別の区間に対して別のクラス分けが必要になる．記号を入れて整理しよう．

の隣り合う 2 つの区間の最初の数の差のことです[14]．当然のことですが，このような隣り合う区間の 2 番目 (3 番目も，4 番目も，何番目も) の差はまた d_1 に等しいのです．

この区間の列に，ここでさらにその次の $l+1$ 番目の区間 $\Delta_{l'}$ を付け加えると[15]($l' = l+1$ でした)，この区間は区間 Δ の左半分の境界からはみ出すかもしれませんが，ともかく区間 Δ の中にはすっぽりと含まれています．こうなれば区間 $\Delta_1, \Delta_2, \cdots, \Delta_l, \Delta_{l'}$ は長さ q_{k-1} の区間の作る，公差 d_1 の，長さ $l' = l+1$ の等差列になっています．ここで，$\Delta_1, \Delta_2, \cdots, \Delta_l$ は同じタイプなのですが，最後の区間 $\Delta_{l'}$ のタイプについては何も分かりません．これで，構成の最初の段階は終りました．

次に進む前に，どのような構成であったか，もう一度じっくり考えてご覧なさい．

区間 Δ の長さは $|\Delta| = q_k = 2n_{k-1}q_{k-1}$ なので，$\Delta = \{a, a+1, \cdots, a+q_k-1\}$ と書いておく．Δ の左半分は $\{a, a+1, \cdots, a+n_{k-1}q_{n-1}-1\}$ であり，長さ q_{k-1} の区間 $\delta_p = \{a_p, a_p+1, \cdots, a_p+q_{k-1}-1\}$，(ここで，$a_p = a+(p-1)q_{k-1}$，$1 \leqq p \leqq n_{k-1}$) が，$n_{k-1}$ 個並んでいると思ってよい．

ここで，まったく別に区間 $\delta = \{1, 2, \cdots, n_{k-1}\}$ を考え，これをクラス分けする．δ の 2 数 p, q が，$\delta_p \sim \delta_q$，つまり $a_p + i \sim a_q + i$ $(0 \leqq i < n_{k-1})$ であるとき，同じクラスに属すと言い，$p \approx q$ と書く．上の注意により，$\approx$ でのクラスの数は高々 $k^{q_{k-1}}$ なので，$n_k = n(k^{q_{k-1}}, l)$ の意味から (帰納法の仮定から)，$\approx$ でのクラスの少なくとも 1 つには長さ l の等差数列が含まれることになる．その初項を c，公差を d とすれば，$\Delta_1 = \delta_c = \{a_c, a_c+1, \cdots, a_c+q_{k-1}-1\}, \Delta_2 = \delta_{c+d}, \cdots, \Delta_l = \delta_{c+(l-1)d}$ とおけばよい．

$c + id \approx c + jd$ $(0 \leqq i, j < l)$ なのだから，$\delta_{c+id} \sim \delta_{c+jd}$ $(0 \leqq i, j < l)$ となっている．

[14] [訳註] 上の訳註の記号を使えば $d_1 = dq_{k-1}$ である．また，$\mathbb{N}$ の部分集合 A と自然数 $n \in \mathbb{N}$ に対して，$A + n = \{a+n \mid a \in A\}$ と書くことにすれば，$\Delta_{i+1} = \Delta_i + d_1$ となっている．

[15] [訳註] もちろん，等差列になるように．つまり，上の訳註の記号を使えば，$\Delta_{l'} = \Delta_l + d_1 = \{a_{c+ld}, a_{c+ld}+1, \cdots, a_{c+ld}+q_{k-1}-1\}$ とおけばよい．ここでさらに，i $(0 \leqq i < q_{k-1})$ があって，$a_{c+ld} + i \sim a_c + i$ となっているのなら証明は終るのだが，$\Delta_{l'}$ の数のタイプについて，つまり最初に考えた k 個のクラスに $\Delta_{l'}$ の数がどのように分かれているかについては何も分からない．

§5　区間の細分

さて，第 2 段階へ進みましょう．今作った区間列の初めの l 項の中から任意に 1 つ取り，それを Δ_{i_1} $(1 \leqq i_1 \leqq l)$ とします．Δ_{i_1} は長さ q_{k-1} の区間です．区間 Δ と同じように扱うことにします．$q_{k-1} = 2n_{k-2}q_{k-2}$ ですから，区間 Δ_{i_1} の左半分を長さ q_{k-2} の n_{k-2} 個の区間に分けると，この長さの区間に対しては，高々 $k^{q_{k-2}}$ 個の異なるタイプしかありませんが，一方 (1) 式から，$n_{k-2} = n(k^{q_{k-2}}, l)$ となっています．したがって，Δ_{i_1} の左半分には，長さ q_{k-2} の同じタイプの l 個の区間 $\Delta_{i_1 i_2}$ $(1 \leqq i_2 \leqq l)$ の等差列が含まれます．この列の公差 (隣り合った 2 つの区間の最初の数の間の距離) を d_2 とします．この区間列にも $l+1$ 番目の項 $\Delta_{i_1 l'}$ を付け加えますが，もちろんタイプについては何も分かりません．区間 $\Delta_{i_1 l'}$ は，区間 Δ_{i_1} の左半分にはもう含まれないかもしれませんが，区間 Δ_{i_1} 自身には明らかに含まれています．

これまでは 1 つの区間 Δ_{i_1} でだけ構成をしてきましたが，今度は他のすべての区間 Δ_{i_1} $(1 \leqq i_1 \leqq l')$ にこの構成を移すことにします[16]．こうして 2 重添字の区間の族 $\Delta_{i_1 i_2}$ $(1 \leqq i_1 \leqq l', 1 \leqq i_2 \leqq l')$ が得られます．この際明らかに，この区間族の，添字が l を越えない 2 つの任意の区間は，互いに同じタイプです．つまり，

$$\Delta_{i_1 i_2} \sim \Delta_{i'_1 i'_2} \qquad (1 \leqq i_1, i_2, i'_1, i'_2 \leqq l)$$

となっています．

こうなれば貴方には明らかに思えるでしょうが，このプロセスは次々と続けていくことができます．k 回やったとしましょう．

第 1 段階の構成では長さ q_{k-1} の区間が得られ，第 2 段階では長さ q_{k-2} の，などなどとなっています．k 段階の後では長さ $q_0 = 1$ の区間が得られ

---

16 ［訳註］$1 \leqq i'_1, i_2 \leqq l'$ に対して，$\Delta_{i'_1 i_2} = \Delta_{i_1 i_2} + (i'_1 - i_1)d_1$ とおくということである．

る，つまり元々の区間 Δ の数になってしまいますが，それでもこれまで通りこの数を

$$\Delta_{i_1 i_2 \cdots i_k} \qquad (1 \leqq i_1, i_2, \cdots, i_k \leqq l')$$

と書いておきます．この際，$1 \leqq s \leqq k$，$1 \leqq i_1, \cdots, i_s,\ i'_1, \cdots, i'_s \leqq l$ に対して

$$\Delta_{i_1 i_2 \cdots i_s} \sim \Delta_{i'_1 i'_2 \cdots i'_s} \tag{2}$$

となっています[17]．

ここで，以下で重要となる 2 つの注意をしておきます．

1)　(2) 式で，$s < k$ であり，$i_{s+1}, i_{s+2}, \cdots, i_k$ が $1, 2, \cdots, l, l'$ の中から勝手に取ってきた添字であれば，数 $\Delta_{i_1 i_2 \cdots i_{s+1} \cdots i_k}$ が区間 $\Delta_{i_1 i_2 \cdots i_s}$ の中で占める位置は，数 $\Delta_{i'_1 i'_2 \cdots i'_s, i_{s+1} \cdots i_k}$ が区間 $\Delta_{i'_1 i'_2 \cdots i'_s}$ の中で占める位置とまったく同じなのです．この 2 つの区間は (2) 式によって同じタイプですから，次のことが分かります．もし

$$\begin{aligned} &1 \leqq i_1, \cdots, i_s,\ i'_1, \cdots, i'_s \leqq l \\ &1 \leqq i_{s+1}, i_{s+2}, \cdots, i_k \leqq l' \quad (1 \leqq s \leqq k) \end{aligned}$$

ならば，

$$\Delta_{i_1 i_2 \cdots i_s i_{s+1}, i_{s+2}, \cdots, i_k} \sim \Delta_{i'_1 i'_2 \cdots i'_s i_{s+1}, i_{s+2}, \cdots i_k} \tag{3}$$

となります．

2)　$s \leqq k, i'_s = i_s + 1$ のときは，区間 $\Delta_{i_1 i_2 \cdots i_{s-1} i_s}$ と $\Delta_{i_1 i_2 \cdots i_{s-1} i'_s}$ は明らかに，第 s 段階の構成では隣りあった区間です．したがって，添字 $i_{s+1}, \cdots, i_k$ が何であっても，数 $\Delta_{i_1 i_2 \cdots i_{s-1} i_s i_{s+1} \cdots i_k}$ と $\Delta_{i_1 i_2 \cdots i_{s-1} i'_s i_{s+1} \cdots i_k}$ は，その隣りあった 2 つの区間の中で同じ位置にあることになります．それゆえ ($i'_s =$

[17] ［訳註］ただちに分かるのは，$|\Delta_{i_1 i_2 \cdots i_s}| = q_{k-s}$ であり，$\Delta_{i_1 i_2 \cdots i_s}$ が i_s に関して公差 d_s の等差列になっていることである．また，i_s だけを動かして考える数列 $\{\Delta_{i_1 i_2 \cdots i_s \cdots i_k} \mid 1 \leqq i_s \leqq l'\}$ は公差 d_s の等差数列になっている (以下の 2) で示しているように．

i_s+1 のときは),

$$\Delta_{i_1 i_2 \cdots i_{s-1} i'_s i_{s+1} \cdots i_k} - \Delta_{i_1 i_2 \cdots i_{s-1} i_s i_{s+1} \cdots i_k} = d_s \tag{4}$$

となります．

§6　ゴール

さて，もうゴールは遠くありません．区間 Δ の $k+1$ 個の数

$$\left.\begin{array}{l} a_0 = \Delta_{l'l'l'\cdots l'} \\ a_1 = \Delta_{1l'l'\cdots l'} \\ a_2 = \Delta_{11l'\cdots l'} \\ \cdots\cdots\cdots\cdots\cdots \\ a_k = \Delta_{111\cdots 1} \end{array}\right\} \tag{5}$$

を考えましょう．区間 Δ は k 個のクラスに分かれていますが，(5) にある数は $k+1$ 個ですので，この数の中に同じクラスに属する 2 つの数があります．それを a_r, a_s $(r<s)$ としますと

$$\Delta_{\underbrace{1\cdots 1}_{r}\underbrace{l'\cdots l'}_{k-r}} \sim \Delta_{\underbrace{1\cdots 1}_{s}\underbrace{l'\cdots l'}_{k-s}} \tag{6}$$

となります．そこで $l+1$ 個の数

$$c_i = \Delta_{\underbrace{1\cdots 1}_{r}\underbrace{i\cdots i}_{s-r}\underbrace{l'\cdots l'}_{k-s}} \quad (1 \leqq i \leqq l') \tag{7}$$

を考えます[18]．この中の最初の l 個の数は (つまり，$i<l'$ のときは)，(3) 式によって同じクラスに属します．最後の数 ($i=l'$ のとき) も，(6) 式によりこれと同じクラスに属します．こうして，(7) の $l+1$ 個の数はすべて互いに同じクラスに属しています．したがって，定理の証明のためにはこれらの数が等差数列をなすこと，つまり，差 $c_{i+1}-c_i$ $(1 \leqq i \leqq l)$ が i に依ら

[18]［訳註］このとき，$c_1 = a_s$，$c_{l'} = a_r$ となっている．

ないことを示せばよいことになりました．

簡単のために $i+1=i'$ とおいて，さらに

$$c_{i,m}=\Delta_{\underbrace{1\cdots1}_{r}\underbrace{i'\cdots i'}_{m}\underbrace{i\cdots i}_{s-r-m}\underbrace{l'\cdots l'}_{k-s}}\quad(0\leqq m\leqq s-r)$$

とおくと，$c_{i,0}=c_i$，$c_{i,s-r}=c_{i+1}$ であり，したがって

$$c_{i+1}-c_i=\sum_{m=1}^{s-r}(c_{i,m}-c_{i,m-1})$$

となります．しかし，(4) 式によって

$$\begin{aligned}c_{i,m}-c_{i,m-1} &= \Delta_{\underbrace{1\cdots1}_{r}\underbrace{i'\cdots i'}_{m}\underbrace{i\cdots i}_{s-r-m}\underbrace{l'\cdots l'}_{k-s}}\\ &\quad-\Delta_{\underbrace{1\cdots1}_{r}\underbrace{i'\cdots i'}_{m-1}\underbrace{i\cdots i}_{s-r-m+1}\underbrace{l'\cdots l'}_{k-s}}=d_{r+m}\end{aligned}$$

となりますので，

$$c_{i+1}-c_i=d_{r+1}+d_{r+2}+\cdots+d_s$$

となるのですが，実際これは i に依りません．これで定理は完全に証明されました．

まったく初等的な構成であっても時にどれほど複雑になり得るかが，分かったでしょう．しかもこれが限界だというわけではありません．次の章で，同じように初等的でありながらずっと複雑な構成を学ぶことになるでしょう．一方で，ファン・デル・ヴェルデンの定理がさらに簡単な証明をもたないかどうかまったく分かりませんし，この方向でのあらゆる研究は喜んで受け入れられるでしょう．

第 2 章

ランダウ–シュニレルマンの仮説とマンの定理

§1　和の数列

貴方はおそらく，**あらゆる自然数は高々4 つの平方数の和である**という，ラグランジュの素晴らしい定理について聞いたことがあるでしょう．それは言い換えると，あらゆる自然数は，それ自身他の数の平方であるか，またはそのような平方の 2 つか，3 つか，4 つかの和になっているということです[1]．今は，この定理の内容を少し新しい形で考える方が都合が良いのです．平方数の列を 0 から始めて書き下すと，

[1] ［訳註］例えば $n = 1 \sim 100$ の数を実際に，4 つ以下の平方の和に書いて確かめてみると，この定理の素晴らしさにわくわくする．

実際に平方の和に書き下そうとする人のためにデータとして，10000 までの平方数の表を解説の附録として挙げておく．これを眺めながら，10000 までの数で遊んで欲しい．

この事実自身はすでにディオファントスが暗示しており，フェルマーもある書簡の中で大体の証明を与えている．ラグランジュの論文は全集の中で見ることができる．この定理の証明は解説第 2 章 §5 に与えておいた．

じつはさらに自然数 n を 4 つの平方数の和で書く書き方がどれだけあるかも知られている．19 世紀のドイツの数学者ヤコビが楕円関数を用いて求めている．ただし，その数は，(1) 式を満たす整数の 4 つ組み (a_1, a_2, a_3, a_4) がどれだけあるかという数の形で求められている．答えは，n の 4 で割れない約数の和の 8 倍である．n が素数ならば $8(n+1)$ 通りである．

例えば 3 の約数は 1 と 3 で，和の 8 倍は 32 である．その 32 通りは $0+(\pm1)^2+(\pm1)^2+(\pm1)^2, (\pm1)^2+0+(\pm1)^2+(\pm1)^2, (\pm1)^2+(\pm1)^2+0+(\pm1)^2, (\pm1)^2+(\pm1)^2+(\pm1)^2+0$ で与えられる．自然数の組合わせとしては，0,1,1,1 の 1 通りであるので，混同しないように．

このことの簡単な証明が［クーラント，フルヴィッツ (1991)］p.67 にある．

$$0, 1, 4, 9, 16, 25, \cdots \qquad (Q)$$

となりますが，この整数列を Q と書き[2]，これとまったく同じものを 4 つ Q_1, Q_2, Q_3, Q_4 として書き下したと考えて見ましょう．さて，Q_1 から任意の数 a_1^2 をとり，Q_2 からも任意の a_2^2，Q_3 からも任意の a_3^2，Q_4 からも任意の a_4^2 をとって，これらの数を足し合わせると，得られた和

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2 \qquad (1)$$

の可能性は

1. 0 ($a_1 = a_2 = a_3 = a_4 = 0$ の場合)
2. 自然数の平方　(数 n の表示 (1) で，a_1, a_2, a_3, a_4 のうち 3 つが 0 で，4 つ目が 0 でない場合)
3. 2 つの自然数の平方の和　(数 n の表示 (1) で，a_1, a_2, a_3, a_4 のうち 2 つが 0 で，残りの 2 つが 0 でない場合)
4. 3 つの自然数の平方の和　(数 n の表示 (1) で，a_1, a_2, a_3, a_4 のうち 1 つが 0 で，残りの 3 つが 0 でない場合)
5. 4 つの自然数の平方の和　(数 n の表示 (1) で，a_1, a_2, a_3, a_4 のうち 4 つすべてが 0 でない場合)

の 5 つです．

このようにして，得られた数 n は 0 であるか，高々4 つの平方数の和に表わされる自然数であり，明らかに，逆に，すべてのこのような自然数は上記のプロセスで書き表わすことができます．

さて，上記のプロセスで (つまり，数列 Q_1, Q_2, Q_3, Q_4 からそれぞれ取り出した 4 つの数を足し合わせて) 得ることのできるすべての自然数 n を，大きさの順に

$$0, n_1, n_2, n_3, \cdots \qquad (A)$$

と並べます ($0 < n_1 < n_2 < n_3 < \cdots$ としています．つまり，上のように作られた数に同じものがあっても，(A) の中にはそのうちの 1 つしか取ってい

[2] ［訳註］「平方=quadratic」の Q をとったもの．

ません). こうすると，ラグランジュの定理は単に，数列 (A) が自然数全体を含んでいるということ，つまり，$n_1 = 1, n_2 = 2, n_3 = 3$ などとなっているということです.

さてこのプロセスを一般化しましょう. 0 から始まる k 個の単調増大な整数列

$$0, a_1^{(1)}, a_2^{(1)}, \cdots, a_m^{(1)}, \cdots \qquad (A^{(1)})$$

$$0, a_1^{(2)}, a_2^{(2)}, \cdots, a_m^{(2)}, \cdots \qquad (A^{(2)})$$

....

$$0, a_1^{(k)}, a_2^{(k)}, \cdots, a_m^{(k)}, \cdots \qquad (A^{(k)})$$

があるとします. 各数列 $A^{(i)}$ $(1 \leqq i \leqq k)$ から任意に 1 つの数を選んで，これら k 個の数を足し合わせます. このようにして得られる数の全体を重複なく大きさの順に並べると同じタイプの新しい数列

$$0, n_1, n_2, \cdots, n_m, \cdots \qquad (A)$$

が得られます. これを与えられた数列 $A^{(1)}, A^{(2)}, \cdots A^{(k)}$ の**和**と言い，

$$A = A^{(1)} + A^{(2)} + \cdots + A^{(k)} = \sum_{i=1}^{k} A^{(i)}$$

と書きます. ラグランジュの定理の内容は，和 $Q + Q + Q + Q$ が自然数全体の列を含んでいるということになります.

おそらく貴方は，**和 $Q + Q$ が 4 で割ると 1 余るような素数 (つまり，$5, 13, 17, 29, \cdots$) をすべて含んでいる**という有名なフェルマーの定理[3]を聞いたことがあるでしょう. またおそらく，ソ連の有名な学者のイワン・マトヴェーエヴィッチ・ヴィノグラードフが次の素晴らしい定理を証明した[4]こ

[3] ［訳註］これはアルベール・ジラールが推測したものをフェルマーが証明したもの.

[4] ［訳註］ヴィノグラードフ (1937). 解説第 3 章 §11 参照. ゴールドバッハの予想の部分的解決にあたる.

とを御存知でしょう．この定理はこの 2 世紀の間偉大な数学者たちが証明しようとして果せなかったものです.「**0 とすべての素数からなる数列**

$$0, 2, 3, 5, 7, 11, 13, 17, \cdots \qquad (P)$$

を P と書くとき[5]，和 $P+P+P$ は十分大きなすべての奇数を含む.」

これらの例をここで述べた目的は，まったく控え目なものでしかありません．その目的とは，貴方に数列の和の概念に慣れてもらうことであり，この概念を使えばいくつかの古典的な数論の定理を簡単かつ便利に定式化できることを示したかったのです[6].

§2　シュニレルマンの不等式

もちろん貴方が気づいているように，これまでのすべての例では，ある数の数列の和が，何かしらの数のクラス (たとえば，すべての自然数，十分大きなすべての奇数，などの) をすべてかほとんどすべてを含んでしまうことを確立しようとしていたのでした．他の似たようなすべての問題での研究目的は，与えられた数列の和が自然数全体の中である意味で**稠密**であることを示すことです．この際しばしば問題になるのは，この集合が自然数列全体を含んでいる場合です (最初の例ではそうなっていました)．ラグランジュの定理は，数列 Q の 4 つの和が自然数列全体を含むというものです．一般に，同じ数列 A の k 個の和が自然数全体を含むならば，数列 A は (自然数列の) k **次の基底**であるとよぶことになっています．すると，ラグランジュの定理は，平方数の数列 Q が 4 次の基底であるということになります．後に，立方数の数列が 9 次の基底であることが示されました．容易にわかるよう

---

[5] ［訳註］「素数= prime number」の P を取ったもの．

実際に確かめてみようと思う人のために，10000 までの素数を解説の附録の表に書いておく．

[6] ［訳註］これらの胸躍る命題の証明がこの冊子の中にあるものと期待しながらここまで読んで来て，失望を感じるのはおそらく訳者だけではないだろう．フェルマーの定理やラグランジュの定理には初等的な証明が知られているので，それを解説第 3 章で述べることにする．

に，k 次の基底はすべて，$k+1$ 次の基底にもなっています．

これらすべての例，また他の多くの例でも，和の「密度」として知られているものは，足される数列の特定の性質によって，つまりこれらの数列を構成する数の特定の算術的性質 (例えば，平方数であり，素数であり，というような) によって定まっています．1930 年にソビエトの優れた学者であるレフ・ゲンリホーヴィッチ・シュニレルマン[7]は，初めて，いくつかの数列の和の密度は，足される数列の算術的な性質によらず，その密度だけでどの程度まで定まるか，という問題を提出しました．この問題は深くまた興味あるばかりでなく，いくつかの古典的な問題の処理の役に立つことがわかって来ました．多くの優れた研究者たちの努力を引き寄せ，大量の文献を生み出しました．

この分野で問題を厳密に述べ,「密度」という言葉を括弧を付けずに書けるようにするには，何よりも問題の数列の「密度」をどんな数を使って測るのかを取り決めておかねばなりません (ちょうど，物理学において，温度の測り方を学んで初めて,「暖かい」とか「寒い」とかいう言葉に厳密な科学的意味が与えられるようにです)．

数列の「密度」の非常に都合の良い測り方があって，今日では私たちが考えるようなすべての科学的な問題で採用されていますが，それは L.G. シュニレルマンによって提案されたものです．いつものように

$$0, a_1, a_2, \cdots, a_n, \cdots \qquad (A)$$

を単調増加な自然数列，つまり，すべての a_n が自然数で，$a_n < a_{n+1}$, $(n = 1, 2, \cdots)$ を満たす数列とします．数列 (A) の n を越えない自然数の数 (この際 0 は数えません) を $A(n)$ と書くと，$0 \leqq A(n) \leqq n$ となり，その結果

$$0 \leqq \frac{A(n)}{n} \leqq 1$$

となります．明らかにこの分数 $\dfrac{A(n)}{n}$ は，違う n に対して違う値をとりますが，1 から n までという自然数の区間の上での数列 (A) の平均的な密度

---

[7]［訳註］シュニレルマン (1930).

のように考えることができます．この分数の値全体の下限[8]を (全自然数列に関する) 数列 (A) の**密度**とよぶことが，シュニレルマンの提案でした．この密度を $d(A)$ と書きましょう．この概念の簡単な性質を習得するために，以下の命題を自分で証明してみることを勧めます[9]．

1. $a_1 > 1$ であれば (つまり，数列 (A) が 1 を含まないなら)，$d(A) = 0$ である．
2. $a_n = 1 + r(n-1)$(つまり，数列 (A) が，初項 1，公差 r の等差数列である) ならば，

$$d(A) = \frac{1}{r}$$

である．
3. あらゆる等比数列の密度は 0 に等しい．
4. 平方数の列の密度は 0 に等しい．
5. 数列 (A) が自然数の全体を含む ($a_n = n$, $n = 1, 2, \cdots$) ことは，$d(A) = 1$ と必要十分である．
6. $d(A) = 0$ であって，数列 (A) が 1 を含むならば，任意の $\varepsilon > 0$ に対して幾らでも大きな数 N で，

$$A(N) < \varepsilon N$$

を満たすものが存在する．

もしもこれらを貴方が証明したとすれば，密度の概念にも十分慣れ，扱えるようになっているでしょう．さて，次の素晴らしくとても単純な**シュニレルマンの補題**

$$d(A+B) \geqq d(A) + d(B) - d(A)d(B) \tag{2}$$

[8] ［訳註］下限の定義や性質は，大学の微積分の講義で扱われることが多く，最小値の概念を一般化したものである．正確な定義は解説第 2 章 §1 で与える．

[9] ［訳註］ここに証明を補うと訳註だけのページができてしまうので，これらの命題の証明は解説第 2 章 §1 で与えることにするが，できるだけそれを見ずに証明することをお勧めする．

の証明を貴方に紹介したいと思います．この不等式の意味は分かりやすいものです．**任意の 2 つの数列の和の密度は，それらの密度の和から密度の積を引いたものより小さくない**ということです．この「シュニレルマンの不等式」は，和の密度をそれぞれの密度から評価するための，まだ粗っぽいけれど，初めての道具になっています．さて，その証明です．$A(n)$ を数列 A に属する n を越えない自然数の数を表わすとし，$B(n)$ を数列 B に対する同様の数とし，簡単のために，$d(A)=\alpha$, $d(B)=\beta$, $A+B=C$, $d(C)=\gamma$ とおきましょう．自然数の区間 $[1,n]$ は数列 A の $A(n)$ 個の数を含んでいますが，そのおのおのの数は数列 C にも含まれます[10]．a_k と a_{k+1} をそのうちの連続した 2 数とします．その間には，$a_{k+1}-a_k-1=l$ 個の，A に属さない数があり，それは

$$a_k+1,\ a_k+1,\ \cdots,\ a_k+l=a_{k+1}-1$$

です．このうちのいくつかは C にも属しますが，例えば，a_k+r の形で，r が B に属す (このことを簡単に $r\in B$ と書く) ような数はすべて C に属します．しかしこのような数は，区間 $[1,l]$ の中に B の元がどれだけ属するかという数，つまり $B(l)$ 個だけあります．こうして，数列 A の連続した 2 数の間に挟まれた長さ l の区間には少なくとも $B(l)$ 個の C に属する数が含まれています．このことから，区間 $[1,n]$ の C に属する数の個数 $C(n)$ は，少なくとも

$$A(n)+\sum B(l)$$

だけはあります．ここで，和は，A に属する点を除いて得られる区間すべてについて取っています．しかし，密度の定義から $B(l)\geqq\beta l$ なので，

$$C(n)\geqq A(n)+\beta\sum l=A(n)+\beta\{n-A(n)\}$$

となります．なぜなら，$\sum l$ は A に属する点を除いて得られる区間の長さの和なので，単に A に属さない区間 $[1,n]$ の点の個数 $n-A(n)$ となるか

[10] ［訳註］すべての数列は 0 を含んでいることを忘れないように．

らです．しかし，$A(n) \geqq \alpha n$ ですから，

$$C(n) \geqq A(n)(1-\beta)+\beta n \geqq \alpha n(1-\beta)+\beta n$$

となり，これから

$$\frac{C(n)}{n} \geqq \alpha+\beta-\alpha\beta$$

が得られます．この不等式はすべての自然数 n に対して成り立つので，

$$\gamma = d(C) \geqq \alpha+\beta-\alpha\beta$$

が得られて，証明が終ります．

シュニレルマンの不等式 (2) はこれと同値な

$$1-d(A+B) \leqq \{1-d(A)\}\{1-d(B)\}$$

という形に書くこともできて，この形なら任意個数の数列の場合にも

$$1-d(A_1+A_2+\cdots+A_k) \leqq \prod_{i=1}^{k}\{1-d(A_i)\}$$

と容易に一般化することができます．証明は単純な帰納法でできるので，自分でやってみても難しくないでしょう．最後の不等式を

$$d(A_1+A_2+\cdots+A_k) \geqq 1-\prod_{i=1}^{k}\{1-d(A_i)\} \tag{3}$$

の形に書けば，また和の密度をそれぞれの密度で評価する可能性を与えています．L.G. シュニレルマンは，自分の初等的な不等式からとても素晴らしい一連の結果，とりわけ次の重要な定理を導き出しました．

あらゆる正の密度の数列は自然数列の基底となる．

言い換えれば，もし $\alpha = d(A) > 0$ ならば，数列 A の十分たくさんの和は自然数全体を含むということです．この定理の証明はとても簡単なので，

私たちが直接問題にしていることからは少しはずれてしまいますが，お話しておきたいと思います．

それぞれが A と一致する k 個の数列の和を，簡単のために，A_k と書くことにすれば，不等式 (3) によって

$$d(A_k) \geqq 1-(1-\alpha)^k$$

が得られ，$\alpha > 0$ ですから，十分大きな k に対して

$$d(A_k) > \frac{1}{2} \tag{4}$$

となります．

さて，数列 A_{2k} が自然数全体を含むことを容易に証明できるようになりました．このことは単に，次の一般的な命題から導かれます．

補題． **もし** $A(n)+B(n)>n-1$ **ならば，**n **は** $A+B$ **に属する．**

実際，もし n が A か B かに属せば，証明が終っています．そこで，n は A にも B にも属していないと仮定しても構いません．そのとき，$A(n)=A(n-1)$，$B(n)=B(n-1)$ であり，したがって

$$A(n-1)+B(n-1)>n-1$$

となっています．

区間 $[1,n-1]$ の A と B に属する数をそれぞれ $a_1,a_2,\cdots,a_r$ と $b_1,b_2,\cdots,b_s$ とします．すると，$r=A(n-1)$，$s=B(n-1)$ です．そのとき，

$$a_1,a_2,\cdots,a_r$$

$$n-b_1,n-b_2,\cdots,n-b_s$$

という数はすべて区間 $[1,n-1]$ に属します．これらの数の数は $r+s=A(n-1)+B(n-1)>n-1$ なので，上の列のどれかの数は下の列のどれかの数と同じになります．それを $\alpha_i=n-b_k$ とすると，$n=a_i+b_k$ とな

り，つまり，n は $A+B$ に属することになります．

さて，以前の考察に戻って，(4) を使えば，任意の n に対して

$$A_k(n) > \frac{1}{2}n > \frac{1}{2}(n-1)$$

となっているので，

$$A_k(n) + A_k(n) > n - 1$$

となります．これから，証明したばかりの補題を使えば，n は $A_k + A_k = A_{2k}$ に属します．しかし，n は任意の自然数だったのですから，定理が証明されたことになります．

この簡単な定理から，L.G. シュニレルマンの論文で，一連の重要な命題が導かれています．そうですね，1 とすべての素数からなる数列が自然数列の基底になることを最初に示したのは彼です．確かに，この数列 P は，すでにオイラーが証明したように密度が 0 ですから[11]，今証明したばかりの定理を直接に適用することはできません．しかし，シュニレルマンは $P+P$ が正の密度を持つことを証明することに成功しました[12]．つまり，$P+P$ が，したがって P が実際に基底になっています．このことから，十分大きな k を取れば，1 以外のどんな自然数も k 個以下の素数の和として表わすことができることが，容易に結論されます．その当時 (1930 年) この結果は基本的なものであり，科学の世界で大きな関心を集めました．I.M. ヴィノグラードフの優れた研究のおかげで，この章の最初ですでにお話ししたように，今日ではこの方面についてかなり多くのことがわかっています．

---

[11] ［訳註］解説第 2 章 §2.3 で証明を与える．§1 では P は 1 を含まなかったが，今は密度の議論をするため，1 を含んでいないと議論が自明になってしまう．以降は P が 1 を含んでいることに注意する．

[12] ［訳註］1930 年のこと．この証明は現在でもやさしくない．

§3　シュニレルマンの不等式の改良

これまで述べて来たのは，L.G. シュニレルマンの素晴らしい仕事から始まった，数論の独特で魅力的な領域に，できるだけ短い道で貴方を誘いたいということでした．しかしながら，もともと本章で目的としたのはこの領域のある特定の問題でした．これからその問題の定式化に移ることにしましょう．

1931 年の秋，外国出張から帰って来たばかりの L.G. シュニレルマンは，ゲッティンゲンでのランダウと討論したことを話してくれましたが，とりわけ，討論をしている中で次のような興味深い事実を確認したことを報告してくれました．彼らが考えつくあらゆる具体的な例では，§2 で証明した不等式

$$d(A+B) \geqq d(A)+d(B)-d(A)d(B)$$

を，もっと強力 (で，もっと簡単) な不等式

$$d(A+B) \geqq d(A)+d(B) \tag{5}$$

におき換えることができるというのです．つまり，和の密度は常に少なくともそれぞれの密度の和だけはあるのです (もちろん，$d(A)+d(B) \leqq 1$ という条件があってのことですが)．したがって彼らは，自然なこととして，不等式 (5) が一般に成り立つ規則であると考えました．しかしこの仮説を証明しようとやってみたことは取りあえずすべてうまく行かなかったのです．この仮説が正しいとしても，その証明への道はいずれにしても大変難しいものになるだろうということが，まもなく明らかになってきたのです．ここで注意しておきたいのは，この仮説の不等式 (5) が実際に一般法則であったなら，この法則は数学的帰納法を使って任意個数の和の場合に拡張される，つまり，$\sum_{i=1}^{k} d(A_i) \leqq 1$ の条件のもとで，不等式

$$d\left(\sum_{i=1}^{k} A_i\right) \geqq \sum_{i=1}^{k} d(A_i) \qquad (6)$$

が成り立つということです．このように提出された問題は，仮説の一般法則 (5) の単純さや優美さのおかげで， 自然に研究者たちの注意を引かずにはおきませんでしたが，それはまた，問題が初等なことと最初の段階ですでに明らかになった解決の困難さとの際だった対照のせいでもありました．私自身もこれに大変惹きつけられ，そのため他の研究はすべて放り出してしまいました．数ヶ月の間頑張って仕事をした結果，1932 年の初めに，$d(A) = d(B)$ というもっとも重要な場合に対して，不等式 (5) を証明することに成功しました (大半の具体的な問題では足される数列は単に互いに同じものであるという理由で，この場合がもっとも重要だとみなすべきものなのです)．同時に私は，$d(A_1) = d(A_2) = \cdots = d(A_n)$ という仮定のもとで一般的な不等式 (6) を証明しました (この結果は，簡単にわかることですが，上の結果から単純な帰納法で得ることはできず，そのための証明が別に必要です)．私が使った方法は完全に初等的なものでしたが大変複雑なもので，後になって証明をいくぶん簡単にすることはできました[13]．

そうだとしても，これは結局部分的な場合にすぎません！ あまり複雑に改良しなくても，私の方法で問題の完全な解答が得られるように，かなり長い間思っていたのですが，こうした方向ではどう努力しても成果が得られませんでした．

そのうち私の仕事が出版され，すべての国の研究者の広い層の注意がランダウ–シュニレルマンの仮説に向けられるようになりました．あまり意味のない部分的な結果がたくさん得られ，この問題の文献というジャンルまで生まれました．何人かの著者は，この問題を自然数の領域から別の領域に移してみせました．一言で言えば，問題は「流行る」ようになったのです．学会は懸賞問題にしました．1935 年のイギリスの友人からの手紙に，イギリスの数学者の大半は当面の仕事をそっちのけにして，この問題を解こうとして

[13] ［訳註］このほかにも，1936 年にヒンチンとエルデシュは，$d(B) = 0$ であっても B が自然数の基底になっていれば，$d(A+B) > d(A)$ となることを示している．

いると書いてあります．ランダウは，加法的整数論の最近の成果に捧げられたその著書の中で,「読者の心にこの問題を刻み込み」たいものだと書いています．しかし問題はとても頑強に抵抗し，なおも数年の間，もっとも有能な研究者たちの努力にも屈しなかったのです．やっと 1942 年になって，アメリカの若い数学者であるマンが，ついにこれを克服しました．彼は，不等式 (5) の (そしてまた不等式 (6) の) 完全な証明を発見したのです．彼の方法はまったく初等的で，私の仕事の方法に近いスタイルではありましたが，まったく異なったアイデアに基づいていました．証明は大変複雑で長いものなので，それをここで貴方に書こうとは思いません．しかし 1 年後の 1943 年に，アルティンとシェルクはこの定理のまったく別のアイデアに基づいた新しい証明を出版しました[14]．それは，かなり見通しが良くて短く，以前のもののようにまったく初等的なものでした．それで，これが貴方にお話ししようと思うものなのです．そのために私はこの章を書いてきましたし，以下の節はすべてこの証明なのです．

§4　基本補題

それでは，A と B を 2 つの数列とし，$A+B=C$ とおきます．$d(A)$, $d(B)$ なども意味はいつもの通りとします．考えている数列はいつも 0 から始まるけれど，$A(n)$, $B(n)$, $C(n)$ を計算する際にはこれらの数列に属する自然数だけを問題にすることにしていたことを思い出しておきましょう．$d(A)+d(B) \leqq 1$ という条件のもとで不等式

$$d(C) \geqq d(A)+d(B) \tag{7}$$

が成り立つことを証明しなければなりません．以下，簡単のために，$d(A)=\alpha$, $d(B)=\beta$ とおきましょう[15]．

基本補題．　任意の自然数 n に対して，

---

[14] ［訳者］［アルティン，シェルク (1943)］．アルティン全集の p.346-350 に再録されている．

[15] ［訳註］忘れがちになるが，第 2 章の終るまで，$\alpha+\beta \leqq 1$ は仮定されている．

$$C(n) - C(n-m) \geqq (\alpha+\beta)m$$

を満たす数 m $(1 \leqq m \leqq n)$ が存在する．

言いかえれば，区間 $[1,n]$ には，数列 C のそこでの平均密度が $\alpha+\beta$ より小さくないような「端」$[n-m+1,n]$ があるということです．

ここで 2 つの問題が生まれます．1) 基本補題を証明することと，2) 基本補題から不等式 (7) を導くことです．このうち 2 番目の問題の方がはるかにやさしいので，そちらから始めましょう．

さて，基本補題は証明されているとします．区間 $[1,n]$ のある「端」$[n-m+1,n]$ では，数列 C の平均密度が $\alpha+\beta$ より小さくないとします．しかし，区間 $[1,n-m]$ にも，基本補題によって，そこでの C の平均密度が $\alpha+\beta$ より小さくないような「端」$[n-m-m'+1,n-m]$ があります．この議論を続けていくと，明らかに有限回で，区間 $[1,n]$ の有限分割で，その各々の部分区間では C の平均密度が $\alpha+\beta$ より小さくないようなものが得られます．つまり，区間 $[1,n]$ の全体で数列 C の平均密度は $\alpha+\beta$ より小さくありません．さらに，数 n は任意でしたから，

$$d(C) \geqq \alpha+\beta$$

となり，これが証明すべきことでした．

こうして，問題は基本補題の証明に帰着しました．長くて複雑なこの証明を，今から始めることにしましょう．

§5　正規数列

以下の全体で，数 n は固定され，以下に考察する数列は数 0 と区間 $[1,n]$ の中の数からなるものとします．ある数列 N [16]は，条件「N に属さない区間 $[1,n]$ の任意の数 f, f' に対して，数 $f+f'-n$ もまた N に属さない (この際，$f=f'$ という場合を除いていません)」を満たすとき，**正規**であ

[16] ［訳註］「正規=normal」の N を取ったもの．

るとよぶことにします[17].

n が 数列 C に属していれば,

$$C(n)-C(n-1)=1\geqq(\alpha+\beta)\cdot 1$$

となって，基本補題は明らかに成り立ちます ($m=1$ として). そこで，以下ではずっと — お願いです，忘れないでください — n は C に属していないものと仮定します.

まずもってわかることは，数列 C が正規であるときは，基本補題は大変簡単に証明できるということです．実際，m を C に属さない最小の自然数とします (n が C に属していないので，$m\leqq n$ です). s を $n-m$ と n の間の任意の数，つまり，$n-m<s<n$ であるとします．すると，$0<s+m-n<m$ となります．$s\in C$ が成り立ちます．実際，もしもそうでなければ，正規性から，数 $s+m-n$ は C に属せません．しかしこの数が m より小さいことは示したばかりで，一方，定義によって，m は C に属さない**最小**の自然数なのです.

こうして，区間 $n-m<s<n$ のすべての数 s は C に属すので,

$$C(n)-C(n-m)=m-1$$

となります.

一方，m は $C=A+B$ に属さないので，§2 の補題によって，$A(m)+B(m)\leqq m-1$ となります．したがって,

$$C(n)-C(n-m)\geqq A(m)+B(m)\geqq(\alpha+\beta)m \tag{8}$$

となって，基本補題の証明が得られたことになります[18].

---

[17] [訳註] 例えば，$\{1,2,\cdots,n-1\}$ は正規である．この集合に属さない数は n だけで，$n+n-n=n$ は確かに属していない.

[18] [訳註] $m=1$ のとき，(8) 式は $0\geqq\alpha+\beta$ となって矛盾するように見える．しかし，$m=1$ ということは，$1\notin C=A+B$ であり，和の定義から，$1\notin A,B$ であり，密度の性質の 1. から，$\alpha=\beta=0$ になる．また $m=1$ のときは上の議論の s は存在していない.

§6　標準拡大

さて，数列 $C = A + B$ が正規性を持たない場合に移りましょう．この場合，集合 B に，ある決まった方法で，B に属していない新しい数をつけ加えて，B から拡大した集合 B_1 に移ることにします．集合 $A + B_1 = C_1$ は明らかに，集合 C の拡大になっています．上で述べたように，集合 B, C のこれらの拡大は (A は変わらないままです)，一意的に定義されることになりますが，それは集合 C が正規でないとき，またそのときに限って可能なものになります．この拡大を，集合 B, C の**標準拡大**とよびます．以下では，標準拡大のいくつかの重要な性質を導き，その助けを借りて基本補題の証明を完成させましょう．

集合 B, C の標準拡大の厳密な定義を与えます．C が正規でなければ，区間 $[0, n]$ には

$$c \notin C,\ c' \notin C,\ c + c' - n \in C$$

を満たす 2 つの数 c, c' が存在します．$C = A + B$ であるので，これから

$$c + c' - n = a + b \quad (a \in A,\ b \in B) \tag{9}$$

が得られます．(9) の形の等式が成り立つような可能なあらゆる数 $b \in B$ の中で最小の数を β_0 とします．言い換えると，β_0 は，区間 $[1, n]$ の数を，$c \notin C$, $c' \notin C$, $a \in A$ を満たすように適当に選ぶとき関係式 (9) を満たすような数 $b \in B$ のうちの最小の数のことです．この数 β_0 をこの拡大の**基**とよびましょう．

こうして，方程式

$$c + c' - n = a + \beta_0 \tag{10}$$

には，

$$c \notin C,\ c' \notin C,\ a \in A$$

を満たし，3 数ともが区間 $[1,n]$ に属するような数 c, c', a の解が存在します．方程式 (10) と上に挙げた条件を満たす c と c' を集めて集合 C^* とします．明らかに，集合 C と C^* は 1 つも共通の元を持ちません．これを足した (つまり，C か C^* に属すすべての数の全体)

$$C \cup C^* = C_1$$ [19]

を，集合 C の**標準拡大**とよびましょう．

さて，表示 $\beta_0 + n - c$ を考えましょう．ここで，c が今作った集合 C^* のすべての数の間を走り回るとすれば，この表示の値はある集合 B^* を作ります．この際，方程式 (10) のおかげで，このような数 $\beta_0 + n - c$ $(c \in C^*)$ は $c' - a$ $(c' \in C^*, a \in A)$ の形に表わすことができます．

b^* を B^* に属す任意の数とします．$\beta_0 + n - c$ の形をしているので $b^* \geqq \beta_0 \geqq 0$ となります．また，$c' - a$ $(c' \in C^*, a \in A)$ の形をしているので $b^* \leqq c' \leqq n$ となります．こうして，集合 B^* のすべての数は区間 $[0,n]$ に属します．その上，$b^* \in B^*$ なら $b^* \notin B$ となります．というのは，もしそうでないなら，$b^* = c' - a$ から $c' = a + b^* \in A + B = C$ となりますが，これは成り立たないからです．

それで，集合 B^* は区間 $[0,n]$ にあって，集合 B と共通な元を持ちません．

$$B \cup B^* = B_1$$

とおき，集合 B_1 を集合 B の**標準拡大**とよびましょう．

まず

$$A + B_1 = C_1$$

であることを示しましょう．

まず $a \in A$, $b_1 \in B_1$ として，$a + b_1 \in C_1$ を示します．$b_1 \in B_1$ から，$b_1 \in B$ か $b_1 \in B^*$ かのどちらかです．$b_1 \in B$ なら，$a + b_1 \in A + B =$

---

[19] ［原註］これ以降，集合の和に対して $\cup$ という記号を使う．

$C \subset C_1$ です．$b_1 \in B^*$ なら，$a + b_1 \in C$ つまり C_1 の元であるか，$a + b_1 \notin C$ であるかのどちらかです．後者の場合は (b_1 は集合 B_1 の元であることから，$\beta_0 + n - c'$, $c' \notin C$ の形をしているので)，

$$c = a + b_1 = a + \beta_0 + n - c' \notin C$$

となります．こうして

$$c + c' - n = a + \beta_0 \in A + B = C$$

となりますが，$c \notin C$, $c' \notin C$ となっています．しかしそのときは，集合 C^* の定義によって

$$c = a + b_1 \in C^* \subset C_1$$

となり，これが示すべきことでした．つまり，$A + B_1 \subset C_1$ が証明できました．

逆の関係を証明するために，$c \in C_1$ としましょう．すると，$c \in C$ か $c \in C^*$ かになります．$c \in C$ であれば $c = a + b$, $a \in A$, $b \in B \subset B_1$ となります．$c \in C^*$ であれば，ある $a \in A$ に対して数 $b^* = c - a$ は B^* の元になることがわかっています．それだから，$c = a + b^* \in A + B^* \subset A + B_1$ となります．こうして $C_1 \subset A + B_1$ が得られましたが，前に証明したように $A + B_1 \subset C_1$ でしたから，$C_1 = A + B_1$ となります．

さて，思い出して欲しいのですが，$n \notin C$ と仮定していました．これから容易に分かるのですが，そして以下で重要なことなのですが，数 n は標準拡大には属しません．実際，$n \in C^*$ の場合，C^* の定義によって，関係式 (10) で $c' = n$ とおいてもよいことになって，$c = a + \beta_0 \in A + B = C$ となり，その一方で式 (10) の意味から $c \notin C$ なのですから．

拡大した数列 C_1 がまだ正規になっていないならば，$A + B_1 = C_1$ で $n \notin C_1$ なのですから，集合 A, B_1, C_1 の全体はそれ自身，A, B, C の 3 つ組が持っていた，新しい標準拡大のために必要な性質を備えた 3 つ組になっています．

この拡大の新しい基 β_1 を見つけて，補充する集合 B_1^*, C_1^* を前と同じ

ように定義して

$$B_1 \cup B_1^* = B_2, \quad C_1 \cup C_1^* = C_2$$

とおけば，また $A + B_2 = C_2$ で $n \notin C_2$ であることを示すことができます．このプロセスは拡大の集合が正規になるまでは続けることができます．何回かすれば明らかにこのことは起こります．

というのも，それぞれの拡大の際に，集合 B_μ, C_μ に新しい数を付け加えていくけれど，区間 $[0, n]$ という枠からはみ出さないのですから．

このようにして，集合の有限列

$$B = B_0 \subset B_1 \subset \cdots B_h$$
$$C = C_0 \subset C_1 \subset \cdots C_h$$

が得られます．このとき，$B_{\mu+1}$ と $C_{\mu+1}$ はそれぞれ，B_μ と C_μ に入らない数を含み，そのような数は B_μ^* と C_μ^* を作り，

$$B_{\mu+1} = B_\mu \cup B_\mu^*, \quad C_{\mu+1} = C_\mu \cup C_\mu^* \quad (0 \leqq \mu \leqq h-1)$$

となっています．この際，(B_μ, C_μ) から $(B_{\mu+1}, C_{\mu+1})$ へ移行する拡大の基を β_μ と書きます．結果として

$$A + B_\mu = C_\mu, \quad n \notin C_\mu \quad (0 \leqq \mu \leqq h)$$

が得られ，集合 C_h は正規ですが，集合 C_μ $(0 \leqq \mu \leqq h-1)$ はこの性質を持っていません．

§7　標準拡大の性質

以下で必要となる標準拡大の性質を，3 つの補題にまとめ，証明します．その中で最後のものだけが後に応用されるのです．補題 1 と 2 は補題 3 の証明のために必要なだけです．

補題 1.　$\beta_\mu > \beta_{\mu-1}$ $(1 \leqq \mu \leqq h-1)$，**つまり，次々の標準拡大の基は単調増大数列をなす．**

実際，$\beta_\mu \in B_\mu = B_{\mu-1} \cup B^*_{\mu-1}$ なので，$\beta_\mu \in B_{\mu-1}$ であるか，$\beta_\mu \in B^*_{\mu-1}$ であるかです．$\beta_\mu \in B^*_{\mu-1}$ ならば，β_μ は

$$\beta_\mu = \beta_{\mu-1} + n - c$$

という形をしており，$c \in C^*_{\mu-1} \subset C_\mu$ となっています．$c < n$ なのだから $\beta_\mu > \beta_{\mu-1}$ となり補題 1 が示されたことになります．$\beta_\mu \in B_{\mu-1}$ の場合は，数 β_μ の定義から，関係式

$$c + c' - n = a + \beta_\mu \in C_\mu$$

を満たす数 $a \in A$, $c \notin C_\mu$, $c' \notin C_\mu$ が存在することを注意しておきます．しかし，$\beta_\mu \in B_{\mu-1}$ なのだから，$c \notin C_{\mu-1}$, $c' \notin C_{\mu-1}$ として

$$c + c' - n = a + \beta_\mu \in A + B_{\mu-1} = C_{\mu-1} \tag{11}$$

となっています．したがって，$\beta_{\mu-1}$ の定義から $\beta_\mu \geqq \beta_{\mu-1}$ です．$\beta_\mu = \beta_{\mu-1}$ だったとすれば，集合 $C^*_{\mu-1}$ の定義によって，(11) 式から

$$c \in C^*_{\mu-1} \subset C_\mu, \quad c' \in C^*_{\mu-1} \subset C_\mu$$

となりますが，左も右も成り立たないので，$\beta_\mu > \beta_{\mu-1}$ となります．

これ以降，C_h に属さない最初の正整数を m と書くことにします．

補題 2.　$c \in C^*_\mu$, $0 \leqq \mu \leqq h-1$ **かつ** $n - m < c < n$ **であれば，**$c > n - m + \beta_\mu$ **となる．つまり，区間** $n - m < c < n$ **の中にある，集合** C^*_μ **のすべての数** c **は，不等式** $n - m + \beta_\mu < c < n$ **で特徴づけられる部分区間の中にある．**

証明しなければならないのは

$$c + m - n > \beta_\mu$$

という関係です．

$n-m<c<n$ から

$$0<m+c-n<m$$

が出ますが，数 m の定義によって

$$m+c-n\in C_h$$

となります．しかし，

$$C_h=C_\mu\cup C_\mu^*\cup C_{\mu+1}^*\cup\cdots\cup C_{h-1}^*$$

であるので，2 つの場合に分かれます．

1)　$m+c-n\in C_\mu$ であれば，

$$m+c-n=a+b_\mu,\ \ a\in A,\ b_\mu\in B_\mu$$

なのですが，$m\notin C_\mu$ であり，$c\notin C_\mu$ です (これは $c\in C_\mu^*$ であることから)．したがって，β_μ の最小性から $b_\mu\geqq\beta_\mu$ とならないといけません．しかし，$b_\mu=\beta_\mu$ の場合は，C_μ^* の定義によって $m\in C_\mu^*$ となりますが，こういうことは起こりません．なぜなら，$C_\mu^*\subset C_\mu\subset C_h$ であって，$m\notin C_h$ であるからです．このため $b_\mu>\beta_\mu$ となり，つまり，

$$m+c-n=a+b_\mu\geqq b_\mu>\beta_\mu$$

となって，補題 2 が証明されます．

2)　$c'=m+c-n\in C_\nu^*,\ \mu\leqq\nu\leqq h-1$ であれば，集合 C_ν^* の定義によって，c' は，$a\in A,\ c''\in C_\nu^*$ として，(10) の型の方程式

$$c'-a=\beta_\nu+n-c''$$

を満たします．これから，$c'\geqq c'-a>\beta_\nu\geqq\beta_\mu$ (最後の不等式は補題 1 による) が得られ，補題 2 がまた証明されます．

補題 3.

$$C^*_\mu(n) - C^*_\mu(n-m) = B^*_\mu(m-1) \quad (0 \leqq \mu \leqq h-1)$$

つまり，区間 $n-m<c<n$ の中の数 $c \in C^*_\mu$ の数は，区間 $0<b<m$ (区間の長さは同じ) の中の数 $b \in B^*_\mu$ の数とちょうど同じである.

関係式

$$b = \beta_\mu + n - c \tag{12}$$

を考えましょう．集合 B^*_μ と C^*_μ の定義により，$c \in C^*_\mu$ から $c \in B^*_\mu$ が導かれるし，逆も成り立ちます．このとき，$n-m+\beta_\mu<c<n$ から $\beta_\mu < b < m$ が得られ，その逆も成り立ちます．こうして

$$C^*_\mu(n) - C^*_\mu(n-m+\beta_\mu) = B^*_\mu(m-1) - B^*_\mu(\beta_\mu)$$

となります[20]．しかし，補題 2 によって，$C^*_\mu(n-m+\beta_\mu) = C^*_\mu(n-m)$ となっています．一方，すべての $b \in B^*_\mu$ は，$c<n$ として，(12) の形に表わされるので，β_μ より大きく，したがって $B^*_\mu(\beta_\mu)=0$ となります．

これから，

$$C^*_\mu(n) - C^*_\mu(n-m) = B^*_\mu(m-1)$$

となりますが，これが証明すべきことでした．

§8　基本補題の証明

§5 の結果により，また今証明したばかりの補題 3 に基づけば，基本補題は今やまったく簡単に証明することができるようになりました．

数列 A, B_h, C_h に，§5 の結果を不等式 (8) の形で使えば (C_h の正規性からこうしてもよい)，

---

20 [訳註] $n \notin C^*_\mu$ であることを忘れないように．

$$C_h(n) - C_h(n-m) \geqq A(m) + B_h(m) \tag{13}$$

が得られます．ここで，m は C_h に属さない最小の正整数です．あきらかに，$m \notin A$, $m \notin B_h$ なので，$A(m)$ と $B_h(m)$ の代わりにそれぞれ，$A(m-1)$ と $B_h(m-1)$ と書いても良いのです．

$$C_h = C \cup C^* \cup C_1^* \cup \cdots \cup C_{h-1}^*$$

$$B_h = B \cup B^* \cup B_1^* \cup \cdots \cup B_{h-1}^*$$

であり，この 2 つの和集合のどちらも，和をとる集合たちは互いに共通な元を持たないので，

$$C_h(n) - C_h(n-m) = C(n) - C(n-m) + \sum_{\mu=0}^{h-1}\{C_h^*(n) - C_h^*(n-m)\}$$

$$B_h(m) = B_h(m-1) = B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1)$$

となります．ここで，もちろん $C_0^* = C^*$, $B_0^* = B^*$ とおいています．これから (13) 式によって，

$$C(n) - C(n-m) + \sum_{\mu=0}^{h-1}\{C_h^*(n) - C_h^*(n-m)\}$$

$$\geqq A(m) + B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1)$$

が得られます．しかし，補題 3 によって

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \quad (0 \leqq \mu \leqq h-1)$$

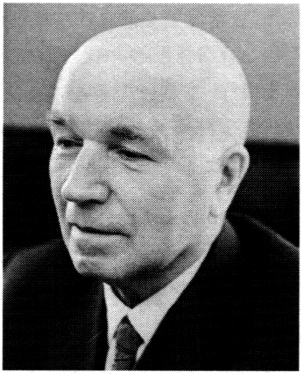
ですから，上の不等式に代入すれば，

$$C(n) - C(n-m) \geqq A(m) + B(m-1) = A(m) + B(m) \geqq (\alpha+\beta)m$$

となり，基本補題の証明が得られました．

こうして，§4 で見たように，加法的整数論の基本的な計量問題を解決するマンの定理は完全に証明されました．

アルティンとシェルクの構成は優れた巨匠の作品という印象がする，と思いませんか？　構造的な繊細さと極めて初等的な方法とのこの素晴らしい結びつきに，私は特に魅きつけられるのです．



ヴィノグラードフ



リニク



ウェアリング

第 3 章

ウェアリングの問題の初等的な解法

§1　ウェアリングの問題

前の章の始めにお話ししたラグランジュの定理を思い出してください．あらゆる自然数は 4 つ以下の平方数の和に書けるというものでした．この定理がまったく別の言葉で表わされるということもお話ししました．つまり，数列

$$0, 1^2, 2^2, \cdots, k^2, \cdots \qquad (A_2)$$

を 4 つ足し合わせればすべての自然数を含む数列が得られるのです．さらにもっと短く，数列 (A_2) は (自然数列の) 4 次の基底である，とも言いました．私はまったく簡単に次のことにも触れました．後に証明されたように，立方数の数列

$$0, 1^3, 2^3, \cdots, k^3, \cdots \qquad (A_3)$$

は 9 次の基底になります．これらの事実を考えれば，自然に，任意の自然数 n に対して，数列

$$0, 1^n, 2^n, \cdots, k^n, \cdots \qquad (A_n)$$

が基底になるという予想を思いつきます (次数はもちろん n によりますが). そして実際，この仮説は 18 世紀にすでにウェアリングが述べています[1]. しかしながら問題はとても難しいもので，やっと今世紀の始めになって (1907 年に) D. ヒルベルトが，ウェアリングの仮説はすべての場合に正しいことを証明しました[2]. ヒルベルトの証明は，形式的な点からも大変雑然としており，複雑な解析的な理論 (多重積分) に基づいているばかりでなく，概念的にもまったく見通しの悪いものでした．フランスの有名な数学者 H. ポアンカレは，ヒルベルトの科学的業績についての概説の中で，「もしもこの証明が働く基本的な機構を何かしら理解したなら，ちょうど豊饒（ほうじょう）の角[3]のように，大きな意味をもつ算術的な結果が，きっと降り注ぐことだろう」と書いています．そしてある意味で彼は正しかったのです．10-15 年経って，イギ

---

[1] [訳註] この次数を $g(n)$ と書くとき，ウェアリング (1770) は $g(2)=4$, $g(3)=9, g(4)=19$ であると予想している．

$g(2)=4$ はラグランジュにより，$g(3)=9$ はヴィーフェリッヒ (1909) によって証明されたが，十分大きな数に対しては 8 つの立方数で表わされることも，ヤコビがある計算家にさせた計算で予想されていた．12000 までに，9 個必要な数は 23 と 239 だけであり，8 個必要なものも 15 個しかない．1939 年にディクソンは $23 = 2\times 2^3 + 7\times 1^3$ と $239 = 5^3 + 3\times 3^3 + 4\times 2^3 + 1$ 以外の整数はすべて 8 個で書けることを示している．

数列 (A_n) の $G(n)$ 個の和がある数より大きいすべての自然数を含むような最小の数として，$G(n)$ を定義すると，一般には $G(n) \leqq g(n)$ であるが，実際に $G(3) \leqq 8 < g(3)$ であることがランダウによって証明されている．

$n=4$ の場合はとても難しく，15 では 15 個，31 では 16 個，47 では 17 個，63 では 18 個，79 では 19 個の 4 乗数が必要で，$g(4) \geqq 19$ が分かる．上からの評価の最初のものはリウヴィルによる $g(4) \leqq 53$ で，$g(2)=4$ を使ったこの評価の初等的な証明が，ラーデマッヘル，テプリッツ (1933) に紹介されている．以降 $g(4)$ の評価は，47,45,41,39,38,37 となっていき，38 を示したランダウの議論の精密化により 37 という評価を示したヴィーフェリッヒの論文 (1909a) の載った雑誌の次の号に，次に述べられるヒルベルトの論文が載っている．

[2] [訳註] ヒルベルト (1909) は，すべての n に対して $g(n)$ が有限であることを証明した．最近，ヒルベルトより 20 年以前に，G.H. ヴンシュトラウムによって，まったく異なるアイデアと方法 (第 2 章の脚注にあるヤコビの方法の拡張) で証明されていたことが報告されている (Math.Intelligencer, vol.8-1(1986), pp.73-74, および vol.8-2, p.79-80 参照).

[3] [訳註] ギリシャ神話で，幼いゼウスに乳を与えたやぎの角のこと．その所有者には，欲しいものが何でも豊富に作り出せるというもの．

リスのハーディーとリトルウッド[4]，そしてソ連のヴィノグラードフ[5]はヒルベルトの定理の新しい証明を与えました．これらの証明もまた解析的であり，形式的にも雑然としたものでしたが，有り難いことにヒルベルトの証明とは違って，方法論的には明快でアイデアも単純なものでしたから，それ以上改良しようという欲求は残らないものでした．実際，このためにどちらの方法も新しい算術の定理を生む力強い源になったのです．

しかし，私たちの科学がウェアリングの問題のようにまったく初等的な問題を扱うときには，初等算術の範囲を逸脱するような概念や方法を必要としないような解法を獲得しようと努力しつづけるものです．ウェアリングの仮説のこのような初等的な証明の探求こそが，貴方にお話ししようとする第3の問題です．ヒルベルトの定理のそのようなまったく初等的な証明は，やっと1942年になって，若いソヴィエトの学者であるYu.V. リニクによって得られました．

貴方はすでに，初等的であることが簡単であることを意味するわけではないことに慣れてきましたね．リニクによって発見されたウェアリングの問題の初等的解法も，これから分かるように，簡単どころではなく，理解し習得

---

[4] [訳註] ハーディーとリトルウッドの，ウェアリングの問題に関する論文 (1920-1928) は文献表に挙げておいたが，彼らが研究を始める時点では $19 \leqq g(4) \leqq 37$，$16 \leqq G(4) \leqq 37$ であることが知られていた ($16 \leqq G(4)$ はケンプナー (1912) による)．彼らは，(1920b) で，$G(4) \leqq 21$ であることを示し，後に $G(4) \leqq 19$ であることを示した．現在は $4 \leqq G(3) \leqq 7$，$G(4) = 16$，$19 \leqq g(4) \leqq 21$ までは知られている．また，チェン (1964) は $g(5) = 37$ であることを証明している．

[5] [訳註] ハーディーとリトルウッドの考え方に沿って， $G(k) \leqq k(6\log k + \log 216)$ という評価 (1935) を，また後に $k \geqq 170000$ なら $G(k) \leqq k(2\log k + 4\log\log k + 2\log\log\log k + 13)$ という評価 (1959) を与えている．またチェン (1958) は $G(k) \leqq k(3\log k + 5.2)$ という評価を与えている．

また一般に $G(k) \geqq k+1$ $(k \geqq 2)$ が知られており，ハーディーとリトルウッドは，k が2のベキのときは $G(k) = 4k$ で，その他のときは $G(k) \leqq 2k+1$ という予想をしている．

1971年のエリッソンの総合報告までに知られていた最良の値は

$$G(2) = 4,\ G(3) \leqq 7,\ G(4) = 16,\ G(5) \leqq 23,\ G(6) \leqq 36,$$
$$G(7) \leqq 52,\ G(8) \leqq 73,\ G(9) \leqq 99,\ G(10) \leqq 122$$

である．

するにはかなりの努力が必要となるでしょう．貴方にとってこの問題ができるだけ簡単になるように説明するつもりです．しかし，覚えておいてもらわないといけないことですが，数学においては (もちろん他のあらゆる科学においても)，本当に価値があり意味のあることを会得するには，どんなことにも，厳しい努力が必要とされるのです．

リニクの証明では，第 2 章の初めに説明したシュニレルマンのアイデアが極めて本質的な役割を果たしています．シュニレルマンが，0,1 とすべての素数からなる数列 P が自然数列の基底になるという彼の有名な定理をどのように証明したかということを，(そこで簡単に述べましたが) 思い出してください．彼は，数列 $P+P$ の密度が正になることを示したのでした．しかし，第 2 章第 2 節で証明を与えたシュニレルマンの一般的な定理によれば，正の密度をもつすべての数列は自然数列の基底になるので，このことからすぐに求めることが得られるのです．この同じ方法が，リニクの発見したヒルベルトの定理の証明の基礎にあるのです．すべてが，数列 (A_n) の十分たくさんの和が正の密度をもつ数列になることの証明に帰着するのです．このことができさえすれば，シュニレルマンの一般的な定理によってヒルベルトの定理は証明されたと考えることができるのです．

§2　基本補題

A_n と同じ k 個の数列を第 2 章の規則で足せば，明らかに，0 と，高々 k 個の x^n の形をした項 (ここで x は任意の自然数) の和として表わされるすべての自然数を含む数列 $A_n^{(k)}$ が得られます．言い換えると，方程式

$$x_1^n + x_2^n + \cdots + x_k^n = m \tag{1}$$

が，非負整数 x_i $(1 \leqq i \leqq k)$ の範囲で解くことができるなら，m は $A_n^{(k)}$ に属すのです．§1 で明らかになったように，私たちの目的は，十分大きな k に対して $A_n^{(k)}$ が正の密度をもつことを証明することです．

与えられた k と m に対する方程式 (1) は，一般に言えば，いろいろな仕

方で解くことができます．以降，その解き方の数，つまり，方程式 (1) を満たす非負整数 $x_1, x_2, \cdots, x_k$ の組の数を，$r_k(m)$ と書きましょう．あきらかに，数 m が $A_n^{(k)}$ に属するのは，$r_k(m) > 0$ のときであり，またそのときに限ります．

以下では，数 n は固定されていると考え，それゆえ，n だけに依存するような数はすべて**定数**であると言いましょう．このような定数を c とか $c(n)$ とかの文字で表わしますが，この際そうした定数 c はあれこれの議論の異なる場所では異なる値をもっているかもしれず，これらの値が定数であるというだけを表わすことにします．このような定数の書き方は，本質的に，証明の際の記法の簡略化なのです．

基本補題． n **にのみ依存する自然数** $k = k(n)$ **と定数** c **が存在して，どんな自然数** N **に対しても**

$$r_k(m) < cN^{\frac{k}{n}-1} \quad (1 \leqq m \leqq N) \tag{2}$$

を満たす．

ここでもまた，前節と同じように 2 つの問題が起きます．第 1 の問題は基本補題を証明することであり，第 2 の問題は基本補題から必要としていた主張，つまり，数列 $A_n^{(k)}$ が正の密度をもつことを導くことです．そしてまた，同じように，第 2 の問題の方が第 1 の問題よりはるかにやさしいので，それから始めることにしましょう．

数 $r_k(m)$ の定義からただちに，その和

$$r_k(0) + r_k(1) + \cdots + r_k(N) = R_k(N)$$

は，

$$x_1^n + x_2^n + \cdots + x_k^n \leqq N \tag{3}$$

を満たす k 個の非負整数 $(x_1, x_2, \cdots, x_k)$ の組の数を表わします．しかし，

$$0 \leqq x_i \leqq \left(\frac{N}{k}\right)^{\frac{1}{n}} \qquad (1 \leqq i \leqq k)$$

を満たす数の集まりはすべてこの要求を満たします．これらの不等式を満たすために，各 x_i は明らかに，$\left(\frac{N}{k}\right)^{\frac{1}{n}}$ より多くの異なる仕方で選ぶことができ $\left(x_i = 0, 1, \cdots, \left[\left(\frac{N}{k}\right)^{\frac{1}{n}}\right]\right)$，これら k 個の選択 (つまり，数 $x_1, x_2, \cdots, x_k$ の選択) は任意の仕方で組み合わされるので，条件 (3) を満たすような数 x_i $(1 \leqq i \leqq k)$ のすべての組には，$\left(\frac{N}{k}\right)^{\frac{k}{n}}$ より多くの異なる選び方があります．これによって，

$$R_k(N) \geqq \left(\frac{N}{k}\right)^{\frac{k}{n}} \tag{4}$$

が得られます．

仮定によって，基本補題は正しく，すべての N に対して不等式 (2) が満たされていることになっています．ここで，不等式 (2) と今証明した不等式 (4) が両立するのは，数列 $A_n^{(k)}$ が正の密度をもつときに限ることを示さないといけません．以下の議論のアイデアはとても単純なものです．和 $R_k(N)$ の中で，m が $A_n^{(k)}$ に属せば，項 $r_k(m)$ は 0 ではありません．もし $A_n^{(k)}$ の密度が 0 ならば，N が大きいときこのような項の数は比較的小さくなります．しかし，(2) のおかげで，各項は大きくなれず，その和である $R_k(N)$ も比較的小さなものになりますが，一方 (4) のおかげでそれは十分大きくないといけません．

あとは計算を実行するだけです．$d(A_n^{(k)}) = 0$ であれば，どれほど小さな $\varepsilon > 0$ に対しても，適当に選んだ N に対して不等式

$$A_n^{(k)}(N) < \varepsilon N$$

が成り立ちます．この際，数 N は好きなだけ大きいとしても構いません．というのは，$A_n^{(k)}$ は (任意の k に対して) 数 1 を含んでいるからです (貴方が証明したはずの第 2 章第 2 節の命題 6 参照)．評価 (2) を使えば，

$$
\begin{aligned}
R_k(N) &= \sum_{m=0}^{N} r_k(m) = r_k(0) + \sum_{m=1}^{N} r_k(m) \\
&< 1 + cN^{\frac{k}{n}-1} A_n^{(k)}(N) < 1 + c\varepsilon N^{\frac{k}{n}}
\end{aligned}
$$

となり[6]，つまり，十分大きな N に対して

$$
R_k(N) < 2c\varepsilon N^{\frac{k}{n}}
$$

となります．十分小さな $\varepsilon > 0$ に対して

$$
2c\varepsilon < \left(\frac{1}{k}\right)^{\frac{k}{n}}
$$

となるので，

$$
R_k(N) < \left(\frac{N}{k}\right)^{\frac{k}{n}}
$$

が得られますが，これは不等式 (4) と矛盾します．こうして

$$
d(A_n^{(k)}) > 0
$$

でなければならず，上に注意したように，ヒルベルトの定理が証明されたことになります．

すべてが単純になっていることが分かったでしょう．しかし，まだ基本補題の証明が残っています．このため，前章でと同じように，長く困難な道を行かねばなりません．

§3　線形方程式に関する補題

基本補題を証明するために，一連の準備のための命題を示しておく必要があります．

---

[6] ［訳註］最初の不等式は $r_k(0) = 1$ と $A_n^{(k)}(N) = \#\{m \mid 1 \leqq m \leqq N,\ r_k(m) \neq 0\}$ による．

まず，線形方程式系の整数解の数に関する評価をします．この節の補題は，おそらく，その解答がここで必要とされた問題とは関りなく，それ自身興味あるものになっているでしょう．

補題 1.　方程式

$$a_1z_1 + a_2z_2 = m \tag{5}$$

に於いて，a_1, a_2, m を整数とし，$|a_1| \leqq |a_2| \leqq A$ かつ $(a_1, a_2) = 1$ [7]を満たすとする．そのとき，不等式 $|z_1| \leqq A,\ |z_2| \leqq A$ を満たす方程式 (5) の解の個数は $\dfrac{3A}{|a_2|}$ を越えない．

証明.　$|a_1| \leqq |a_2|$ と $(a_1, a_2) = 1$ という条件から $a_2 \neq 0$ となり，このとき $a_2 > 0$ と考えることができます．というのは，そうでない場合にはあらゆる解で z_2 を $-z_2$ でおき換えれば良いからです．

2 つの場合が起こり得ます．

1)　$a_1 = 0$ の場合．このとき，$(a_1, a_2) = 1$ ですから，$a_2 = 1$ となり，方程式 (5) は

$$z_2 = m$$

の形をしています．この方程式では，z_2 の値は 1 つより多くはなり得ないし，z_1 は区間 $[-A, A]$ の任意の値を取り得るので，全部で $2A + 1 \leqq 3A$ を越えない個数の値を取ります．このため，条件 $|a_1| \leqq |a_2| \leqq A$ を満たす方程式 (5) の解の個数は $3A = \dfrac{3A}{|a_2|}$ を越えず，この場合の補題の主張が証明されたことになります．

---

[7] ［原註］(a_1, a_2) と $(a_1, a_2, \cdots, a_l)$ はそれぞれ，括弧の中の数の最大公約数を表わしています．

［訳註］$a(\neq 0) \in \mathbb{Z}$ の約数は，$b, c \in \mathbb{Z}$ で $a = bc$ となる b または c のこととし，正負双方を考えている．最大公約数は絶対値をとっても同じ，つまり $(a_1, a_2) = (|a_1|, |a_2|)$ としている．また，すべての整数は 0 の約数と考えられ，$(0, a) = |a|\ (a \neq 0), = \infty\ (a = 0)$ となる．

2) $a_1 \neq 0$ の場合．z_1, z_2 と z_1', z_2' を方程式 (5) の 2 つの異なる解とします．そのとき，

$$a_1 z_1 + a_2 z_2 = m$$
$$a_1 z_1' + a_2 z_2' = m$$

という 2 つの式の引き算をすると

$$a_1(z_1' - z_1) = a_2(z_2 - z_2')$$

が得られます．左辺は a_2 で割れなければなりませんが，$(a_1, a_2) = 1$ なので，$z_1' - z_1$ が a_2 で割れなければなりません．$z_1' \neq z_1$ なので[8]，つまり，$|z_1' - z_1|$ は，a_2 の倍数であることから，a_2 以上になります．したがって，方程式 (5) の 2 つの異なる解 z_1, z_2 と z_1', z_2' に対して

$$|z_1' - z_1| \geqq a_2$$

となります．

方程式 (5) の解 z_1, z_2 に対して，z_1 を第 1 項，z_2 を第 2 項とよびましょう．明らかに，方程式 (5) の，条件 $|a_1| \leqq A$, $|a_2| \leqq A$ を満たす解の個数は，区間 $[-A, A]$ に含まれる第 1 項の数 t よりも多くはありません．2 つのこのような第 1 項は互いに a_2 以上は間をおかないといけないことを示しましたが，それから，区間 $[-A, A]$ に属する第 1 項の最大のものと最小のものとの差は $a_2(t-1)$ より小さくありません．一方，この差は $2A$ を越えないので，そのとき，

$$a_2(t-1) \leqq 2A$$
$$t - 1 \leqq \frac{2A}{a_2}$$
$$t \leqq 1 + \frac{2A}{a_2} \leqq \frac{3A}{a_2}$$

---

[8] ［訳註］$z_1' = z_1$ であれば，$a_1, a_2 \neq 0$ から $z_2' = z_2$ となって，等しい解になってしまう．

となります ($a_2 \leqq A$ という条件から，$1 \leqq \dfrac{A}{a_2}$ となるので)．これで補題 1 が証明されました[9]．

補題 2.　**方程式**

$$a_1 z_1 + a_2 z_2 + \cdots + a_l z_l = m \tag{6}$$

に於いて，a_i と m が整数で

$$|a_i| \leqq A \ (1 \leqq i \leqq l), \qquad (a_1, a_2, \cdots, a_l) = 1$$

を満たすとする．そのとき，不等式 $|z_i| \leqq A \ (1 \leqq i \leqq l)$ を満たす，方程式 (6) の解の個数は

$$c(l)\frac{A^{l-1}}{H}$$

を越えない．ここで，H は数 $|a_1|, |a_2|, \cdots, |a_l|$ の中の最大のものであり，$c(l)$ は l だけに依存する定数である．

証明．　明らかに，$l = 2$ のときは，($c(2) = 3$ として) 補題 2 は補題 1 になります．こうして，$l = 2$ のときは補題 2 はすでに証明が済んでいます．そこで，$l \geqq 3$ であり，$l - 1$ 未知数の場合には補題 2 はすでに証明されていると仮定しましょう．数の順序などどうでもいいことなので，$|a_l|$ が数 $|a_1|, |a_2|, \cdots, |a_l|$ の中で最大であると，つまり，$H = |a_l|$ であると仮定しても構いません．

2 つの場合に分かれます．

1)　$a_1 = a_2 = \cdots = a_{l-1} = 0$ の場合．$(a_1, a_2, \cdots, a_l) = 1$ ですから，$|a_l| = H = 1$ となり，与えられた方程式は $\pm z_l = m$ という形になります．

[9] [訳註] 原著は第 3 版ではそれまでの版と違って，補題の命題で，a_1 と a_2 の役割を入れ換えて，証明の 1) を補っている．しかし，2) はそれ以前の版とまったく同じものを使っている．そのため解の個数の評価が $3A/a_1$ になってしまっている．もちろん，どちらでも証明できるのだが，$a_1 \leqq a_2$ だから，より良い評価である $3A/a_2$ を出すように本訳書では書き直してある．

明らかに，この方程式で，未知数 $z_1, z_2, \cdots, z_{l-1}$ は区間 $[-A, A]$ の任意の整数値をとることができ，つまり，全部で $2A+1 \leqq 3A$ より多くない値しかとりません．z_l については1つより多くの値は取り得ないので，不等式 $|z_i| \leqq A$ $(1 \leqq i \leqq l)$ を満たす与えられた方程式の解の個数は

$$(3A)^{l-1} = c(l)A^{l-1} = c(l)\frac{A^{l-1}}{H}$$

を越えません[10]．これで，この場合には補題2が証明されました．

2) 数 $a_1, a_2, \cdots, a_{l-1}$ の中の少なくとも1つが0でない場合．

$$(a_1, a_2, \cdots, a_{l-1}) = \delta$$

とおきます．数

$$\frac{|a_i|}{\delta} \quad (1 \leqq i \leqq l-1)$$

のうちで最大のものを H' と書くことにします．

さて，数 $z_1, z_2, \cdots, z_l$ は与えられた方程式 (6) と不等式 $|z_i| \leqq A$ $(1 \leqq i \leqq l)$ を満たしているとしましょう．

$$\frac{a_1}{\delta}z_1 + \frac{a_2}{\delta}z_2 + \cdots + \frac{a_{l-1}}{\delta}z_{l-1} = m' \tag{7}$$

と，したがって

$$a_1z_1 + a_2z_2 + \cdots + a_{l-1}z_{l-1} = \delta m'$$

とおくと，明らかに，

$$\delta m' + a_lz_l = m \tag{8}$$

であり，

[10] ［訳註］第2項では $c(l) = 3^{l-1}$ であり，第3項では $c(l) = 3^{l-1}H$ であるが，定数であることだけが重要で，個々の値には大した意味がないわりに，きちんと書くと大変なのでこういう記法を使っている．今なら，オーダーの概念を導入して，$= c(l)$ を $\sim$ と書くこともできる．

$$|\delta m'| \leqq \sum_{i=1}^{l-1} |a_i||z_i| \leqq l\delta H'A$$

となって，これから

$$|m'| \leqq lH'A$$

が得られます．

こうしてもし $z_1, z_2, \cdots, z_l$ が方程式 (6) と不等式 $|z_i| \leqq A$ $(1 \leqq i \leqq l)$ を満たせば，整数 m' が存在して，上の数と一緒に方程式 (7) と (8) を満たしますが，このとき $|m'| \leqq lH'A$ となっています．しかし方程式 (8) で，明らかに，$\delta \leqq |a_l|$ かつ $(\delta, a_l) = 1$ (そうでなければ，$(a_1, a_2, \cdots, a_{l-1}, a_l) > 1$ となります) となっています．したがって，(未知数 m', z_l に関する) 方程式 (8) の，$|m'| \leqq lH'A$ かつ $|z_l| \leqq A < lH'A$ を満たす解の個数は，補題 1 によって，$\dfrac{3lH'A}{|a_l|}$ を越えません．この同じ m' に対して，$l-1$ 未知数の方程式に対する補題 2 によって，方程式 (7) は $c(l)\dfrac{A^{l-2}}{H'}$ 個[11]を越えない整数 z_i，$|z_i| \leqq A$ の解をもっています．

これまで述べてきたことを合わせると，明らかに，不等式 $|z_i| \leqq A$，$1 \leqq i \leqq l$ を満たす，方程式 (6) の解 $z_1, z_2, \cdots, z_l$ の個数は

$$\frac{3lH'A}{|a_l|} c(l) \frac{A^{l-2}}{H'} = c(l) \frac{A^{l-1}}{|a_l|} = c(l) \frac{A^{l-1}}{H}$$

を越えません．これで補題 2 が証明されました[12]．

今度は

$$a_1 z_1 + a_2 z_2 + \cdots + a_l z_l = 0 \tag{9}$$

[11] [訳註] ここでは $c(l-1)$ とした方が分かりやすいが，結局定数であることだけに意味があるという立場から，$c(l)$ という記号を使っている．

[12] [原註] きっと貴方は，この等式の鎖の中の記号 $c(l)$ が異なった場所では異なった値をもっていることに気付いているでしょう．この記号のこのような使い方については §2 の初めにあらかじめ注意してあります．

の型の方程式全体の族を考えましょう．ただし，$|a_i| \leqq A$ $(1 \leqq i \leqq l)$ であり，またこれまで通り a_i はすべて整数です．数 A に対し，不等式 $1 \leqq A \leqq B \leqq c(l)A^{l-1}$ を満たす正の数 B をとり[13]，$l > 2$ とします．この族の方程式 (9) 全体にわたる，解 z_i $(|z_i| \leqq B,\ 1 \leqq i \leqq l)$ の数の和を評価しましょう．

1°．最初に，$a_1 = a_2 = \cdots = a_l = 0$ のときの方程式 (9) を別個に考えて (これだって上の族の方程式です！)，不等式 $|z_i| \leqq B$ $(1 \leqq i \leqq l)$ を満たす解の個数を評価しましょう．明らかに，この方程式はどんな数の組 $z_1, z_2, \cdots, z_l$ でも満たされるので，不等式 $|z_1| \leqq B$, $|z_2| \leqq B, \cdots$, $|z_l| \leqq B$ を満たす数の組がどれだけあるかを計算しさえすればいい訳です．区間 $[-B, +B]$ は $2B+1$ 個より多い整数を含まないので，各 z_i は $2B+1$ より多くない異なる値しか取りません．したがって，問題にしている数の組 $z_1, z_2, \cdots, z_l$ の個数は，

$$(2B+1)^l \leqq (3B)^l = c(l)B^l$$

を越えません．しかし，仮定によって $B \leqq c(l)A^{l-1}$ なので，$c(l)B^l = c(l)B^{l-1}B \leqq c(l)(AB)^{l-1}$ となります．こうして，$a_1 = a_2 = \cdots = a_l = 0$ の場合，方程式 (9) は $c(l)(AB)^{l-1}$ を越えない数の解しかもちません．

2°．もし係数 a_i のうちの 1 つでも 0 でないならば，これらの係数の最大公約数 $(a_1, a_2, \cdots, a_l) = \delta$ が存在します．まず $\delta = 1$ とし，$|a_1|, |a_2|, \cdots, |a_l|$ のうちの最大のものを H とします．明らかに，H は区間 $[1, A]$ の中の整数です．つまり，H は A と $A/2$ の間にあるか，$A/2$ と $A/4$ の間か，$A/4$ と $A/8$ の間か，などなどとなっています．要するに，

$$\frac{A}{2^{m+1}} < H \leqq \frac{A}{2^m} \tag{10}$$

を満たすような整数 $m \geqq 0$ が存在します．

[13] ［訳註］叙述の都合上こう書いてあるが，$c(l)$ は定まった定数ではないので，B の条件として意味があるように見えないかも知れない．もちろんその通りだが，$c(l)$ は以下の議論の中で必要なだけということであり，B もそれに応じて取り直すのである．実際にはこの節の終わりになるまで定まらず，気持ちが悪いかも知れないが，我慢して先に進むこと．

$\delta = 1$ で，H が不等式 (10) を満たすような，(9) の型の 1 つの方程式に対して，解 z_i ($|z_i| \leqq B$) の数は，補題 2 によって，

$$c(l)\frac{B^{l-1}}{H} \leqq c(l)\frac{B^{l-1}}{A/2^{m+1}} = \frac{c(l)B^{l-1}2^m}{A}$$

を越えません．

一方，不等式 (10) から

$$|a_i| \leqq \frac{A}{2^m} \qquad (1 \leqq i \leqq l) \tag{11}$$

となります．したがって，つまり，不等式 (10) を満たすような，(9) の型の方程式の数は，条件 (11) を満たす同じ型の方程式の数，つまり

$$\left(2\frac{A}{2^m}+1\right)^l \leqq \left(3\frac{A}{2^m}\right)^l = c(l)A^l 2^{-ml}$$

より大きくなりません．

こうして，$\delta = 1$ で $\dfrac{A}{2^{m+1}} < H \leqq \dfrac{A}{2^m}$ を満たすような，(9) の型のすべての方程式の解 $|z_i| \leqq B$ の数の和は

$$c(l)\frac{B^{l-1}2^m}{A} \cdot c(l)A^l 2^{-ml} = c(l)(AB)^{l-1}2^{-(l-1)m}$$

を越えません．この評価をすべての $m \geqq 0$ に関して足しあげると，次の結論が得られます．$|a_i| \leqq A$ ($1 \leqq i \leqq l$) と $\delta = 1$ を満たすような，(9) の型のすべての方程式の解 $|z_i| \leqq B$ の総数は

$$c(l)(AB)^{l-1}$$

を越えません．

3°. $\delta > 1$ のときの方程式の考えて来た型の解の数を計算することが残っています．この場合，方程式 (9) は，(9) の型の方程式である方程式

$$\frac{a_1}{\delta}z_1 + \frac{a_2}{\delta}z_2 + \cdots \frac{a_l}{\delta}z_l = 0$$

と同等になります．ただし，

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots, \frac{a_l}{\delta}\right) = 1$$

であり，数 A を数 A/δ におき換える必要がありますが．与えた δ を固定すれば，このようなすべての方程式の解 $|z_i| \leqq B$ の数は，2° で示したように

$$c(l)\left(\frac{A}{\delta} \cdot B\right)^{l-1} = c(l)\frac{(AB)^{l-1}}{\delta^{l-1}}$$

を越えません[14]．

後は，この表示を，可能なすべての値 δ $(1 \leqq \delta \leqq A)$ について足しあげるだけです．

こうして，$|a_i| \leqq A$ $(1 \leqq i \leqq l)$ で，a_i のすべてが 0 なわけではないとき，(9) の型のすべての方程式の欲しかった解の個数の和は

$$c(l)(AB)^{l-1}\sum_{\delta=1}^{A}\delta^{-(l-1)} < c(l)(AB)^{l-1} \cdot \frac{l-1}{l-2} = c(l)(AB)^{l-1}$$

という値を越えません[15]．

---

[14] ［原註］A の代わりにもっと小さい数 A/δ を使っているので，仮定の条件 $B \leqq c(l)A^{l-1}$ が壊れている可能性があります．しかし，2° の議論の際にこの条件をどこでも使わなかったので，したがって 2° の結果がこれにはよらないことを，確かめるのは難しくないでしょう．

[15] ［原註］ここで，任意の自然数 q と任意の $A \geqq 1$ に対して成り立つ不等式

$$\sum_{n=1}^{A}\frac{1}{n^{q+1}} < \frac{q+1}{q}$$

を使っています (ここで，$q = l-2$ は，$l > 2$ と仮定しているので，正になります)．簡単な証明を述べておきましょう．$n \geqq 1$ のとき，

$$\begin{aligned}\frac{1}{n^q} - \frac{1}{(n+1)^q} &= \frac{(n+1)^q - n^q}{n^q(n+1)^q} \\ &= \frac{n^q + qn^{q-1} + \cdots + 1 - n^q}{n^q(n+1)^q} > \frac{qn^{q-1}}{n^q(n+1)^q} > \frac{q}{(n+1)^{q+1}}\end{aligned}$$

となり，これから

$$\frac{1}{(n+1)^{q+1}} < \frac{1}{q}\left\{\frac{1}{n^q} - \frac{1}{(n+1)^q}\right\}$$

これと，$a_1 = a_2 = \cdots = a_l = 0$ の場合に対する評価を得た $1°$ の結果を比較すれば，次の結果が得られます．

補題 3. $l > 2$ **かつ** $1 \leqq A \leqq B \leqq c(l)A^{l-1}$ **とする．そのとき，**

$$a_1 z_1 + a_2 z_2 + \cdots + a_l z_l = 0 \tag{9}$$

の型のすべての方程式の解 $|z_i| \leqq B \ (1 \leqq i \leqq l)$ **の解の数の和は，**$|a_i| \leqq A, \ (1 \leqq i \leqq l)$ **のとき，**

$$c(l)(AB)^{l-1}$$

を越えない．

§4　さらに 2 つの補題

基本補題の証明に移る前に，さらに 2 つの特殊な型の補助的な命題を示しておかないといけません．この 2 つはアイデアの点からも形式の点からも非常に単純なものですが，そのすべてを消化しようとすれば，多少は難しく感じるかもしれません．というのも，ここでは，かなり込み入った構造のあらゆる組合わせを数え尽くすということが問題になっているからです．このような抽象的な組合わせの難しさは，それがうまく数学的な記号化ができないことにあるのです．ここでは，記号よりも言葉で語ることが多くならざるを得ないのです．とは言え，もちろん，これは記述の難しさであって，テーマ自体の難しさなのではありません．そこで，私は，ここで生まれる問題と解

が得られます．この不等式に次々と $n = 1, 2, \cdots, A-1$ を代入すれば，

$$\sum_{n=2}^{A} \frac{1}{n^{q+1}} < \frac{1}{q}\left\{1 - \frac{1}{A^q}\right\} < \frac{1}{q}$$

が得られ，これから

$$\sum_{n=1}^{A} \frac{1}{n^{q+1}} < 1 + \frac{1}{q} < \frac{q+1}{q}$$

が得られますが，これが示したいことでした．

答をできる限り具体的に述べるよう努めましょう．

数の有限集合で，ただし，その中に同じものがあってもよいこととしたものを A と書きます[16]．もし数 a が集合 A の中に λ 回現れるのなら，その**重複度**は λ であると言います．$a_1, a_2, \cdots, a_r$ を A の互いに異なる数で，$\lambda_1, \lambda_2, \cdots, \lambda_r$ をそれぞれの重複度とします (つまり，集合 A には $\sum_{i=1}^{r} \lambda_i$ 個の数があります)．B もまたこの型の集合で，互いに異なる数 $b_1, b_2, \cdots, b_s$ を重複度 $\mu_1, \mu_2, \cdots, \mu_s$ で含んでいるとします．c を与えられた数で，x と y を未知数とする方程式

$$x + y = c \tag{12}$$

を考えましょう．x が数の集合 A の数の 1 つで (このことを $x \in A$ と書きます)，y が数の集合 B の数の 1 つである ($y \in B$) ような，この方程式の解 x, y に興味があるのです．もし数 $x = a_i$，$y = b_k$ が方程式 (12) を満たすのなら，求める型の解が $\lambda_i \mu_k$ 個得られます．集合 A に λ_i 個ある数 a_i のどれでも，集合 B に μ_k 個ある数 b_k のどれとでも組み合わすことができます．しかし，$\lambda_i \mu_k \leqq \frac{1}{2}(\lambda_i^2 + \mu_k^2)$ となっています[17]．つまり，$x = a_i$，$y = b_k$ であるような，方程式 (12) の個数は $\frac{1}{2}(\lambda_i^2 + \mu_k^2)$ を越えません．このことから，方程式 (12) のすべての解 $x \in A$，$y \in B$ の個数はその

---

[16] [訳註] これは普通の意味では自然数の集合の部分集合でなく，以下で分かるように集合の要素を重複度も込めて考えるということである．方程式の解の集合を考えるためのものなので，この方が都合が良い．本章の最後まで，集合という言葉はこの意味で使われている．

もちろん普通の意味で集合を理解するようにすこともできるが，そのためには別のもっと大きな集合を用意する必要がある．

[17] [原註]「相乗平均は相加平均を越えない.」一番簡単な証明は次の通り．

$$0 \leqq (\lambda_i - \mu_k)^2 = \lambda_i^2 + \mu_k^2 - 2\lambda_i \mu_k$$

であり，これから

$$2\lambda_i \mu_k \leqq \lambda_i^2 + \mu_k^2$$

が得られます．

和 $\sum \frac{1}{2}(\lambda_i^2+\mu_k^2)$ を越えません．ここで，$a_i+b_k=c$ を満たす添字のあらゆる対 $i,\ k$ に対して和をとる必要があります．λ_i^2 をすべての i について足し，μ_k をすべての k について足せば，和はさらに大きくなります (各 b_k は 1 つの高々1 つの a_i と組合わせせることができるだけだったのだから).

こうして最終的に，方程式 (12) の解 $x\in A,\ y\in B$ の数は

$$\frac{1}{2}\left(\sum_{i=1}^{r}\lambda_i^2+\sum_{k=1}^{s}\mu_k^2\right)$$

を越えません．

一方，方程式

$$x-y=0 \tag{13}$$

を考え，その解 $x\in A,\ y\in A$ の数を数えましょう．明らかにそういう解はそれぞれ $x=y=a_i$ $(1\leqq i\leqq r)$ の形をしています．i を与えると，解は λ_i^2 個あります．というのは，x と y は互いに独立に，A に入っている λ_i 個の a_i のどれと一致してもよいからです．方程式 (13) の解 $x\in A,\ y\in A$ の総数は，こうして，$\sum_{i=1}^{r}\lambda_i^2$ に等しくなります．まったく同じように，この方程式の解 $x\in B,\ y\in B$ の解の数も $\sum_{k=1}^{s}\mu_k^2$ に等しくなります．この結果を上の結果を比べると次の帰結が得られます．

補題 4.　方程式

$$x+y=c,\qquad x\in A,\ \ y\in B$$

の解の数は，方程式

$$x-y=0,\qquad x\in A,\ \ y\in A$$

と

$$x-y=0,\qquad x\in B,\ \ y\in B$$

の解の数の和の半分を越えない．

集合 A と B が一致するという特別な場合には，次が得られます．

系． 方程式

$$x+y=c, \qquad x\in A,\ \ y\in A$$

の解の数は，方程式

$$x-y=0, \qquad x\in A,\ \ y\in A$$

の解の数を越えない．

k と s を任意の自然数とします．$k\cdot 2^s=l$ とおいて，方程式

$$x_1+x_2+\cdots+x_l=c$$

を考えましょう．

$A_1, A_2, \cdots, A_l$ を数の有限集合とし，各 A_i は互いに異なる数 $a_{i1}, a_{i2}, \cdots$ を重複度 $\lambda_{i1}, \lambda_{i2}, \cdots$ で含んでいるとします．そこで，方程式

$$x_1+x_2+\cdots+x_l=c, \quad x_i\in A_i\ (1\leqq i\leqq l) \tag{14}$$

を問題にするのです．

もし

$$x_1+x_2+\cdots+x_{l/2}=x,\ \ x_{(l/2)+1}+\cdots x_l=y$$

($l/2$ は整数) とおけば，方程式は

$$x+y=c$$

の形に書き直され，補題 4 を適用することができます．しなければならないことは，数 x と y がどんな集合に属すのかを調べることだけです．$x_i\in A_i$ $(1\leqq i\leqq l)$ ですから，x は $z_1+z_2+\cdots+z_{l/2}$ の形，ただし $z_i\in A_i$ $(1\leqq$

$i \leqq l/2)$，のどんな数でも良いし，まったく同じように y も同じ形で良いのですが，ただ $z_i \in A_{(l/2)+i}$ $(1 \leqq i \leqq l/2)$ となっているだけです．したがって，補題 4 によって，方程式 (14) の解の数は，次の 2 つの条件 1), 2) のもとでの方程式

$$x - y = 0 \tag{15}$$

の解の数の和の半分を越えません．

1)
$$x = z_1 + z_2 + \cdots + z_{l/2}$$
$$y = z'_1 + z'_2 + \cdots + z'_{l/2}$$

ここで，

$$z_i \in A_i,\ z'_i \in A_i, \quad 1 \leqq i \leqq \frac{l}{2} \tag{16}$$

を満たす．

2)　x と y は同じ形をしていますが

$$z_i \in A_{(l/2)+i},\ z'_i \in A_{(l/2)+i}, \quad 1 \leqq i \leqq \frac{l}{2} \tag{17}$$

を満たす．

双方の場合とも，方程式 (15) は

$$(z_1 - z'_1) + (z_2 - z'_2) + \cdots + (z_{l/2} - z'_{l/2}) = 0 \tag{18}$$

の形に書き換えられます．

こうして，方程式 (14) の解の数は，条件 (16), (17) のもとでの方程式 (18) の解の数の和の半分を越えません．つまり，方程式

$$\sum_{i=1}^{l/2}(z_i - z'_i) = 0, \qquad z_i \in A_i,\ z'_i \in A_i,\ 1 \leqq i \leqq \frac{l}{2} \tag{18$'$}$$

と

$$\sum_{i=1}^{l/2}(z_i - z'_i) = 0, \qquad z_i \in A_{l/2+i},\ z'_i \in A_{l/2+i},\ 1 \leqq i \leqq \frac{l}{2} \tag{18$''$}$$

の解の数の和の半分を越えません．

方程式 (18) の左辺の項の数は $l/2$ で，つまり，最初の方程式 (14) の半分になっています．

$$\sum_{i=1}^{l/4}(z_i - z_i') = x, \qquad \sum_{i=(l/4)+1}^{l/2}(z_i - z_i') = y$$

とおけば，方程式 (18) は

$$x + y = 0$$

の形になり，さらにまた，補題 4 を適用することができます．方程式 (14) から方程式 (18) を導いたように，今度は方程式 (18) から方程式

$$\sum_{i=1}^{l/4}(u_i + u_i' - u_i'' - u_i''') = 0 \tag{19}$$

が得られます．ただし，この方程式の次の (すでに 4 つの) 条件のもとでの解の数の和を考えないといけません．

$$\left.\begin{array}{ll} 1) & u_i, u_i', u_i'', u_i''' \in A_i \\ 2) & u_i, u_i', u_i'', u_i''' \in A_{(l/4)+i} \\ 3) & u_i, u_i', u_i'', u_i''' \in A_{(l/2)+i} \\ 4) & u_i, u_i', u_i'', u_i''' \in A_{(3l/4)+i} \end{array}\right\} \left(1 \leqq i \leqq \frac{l}{4}\right).$$

$l = k \cdot 2^s$ だったので，このプロセスは s 回繰り返すことができます．結果として，明らかに，方程式

$$\sum_{i=1}^{k}\{y_i^{(1)} + y_i^{(2)} + \cdots + y_i^{(2^{s-1})} - y_i^{(2^{s-1}+1)} - \cdots - y_i^{(2^s)}\} = 0 \tag{20}$$

が得られ，このとき，2^s 個の異なる条件

$$\left.\begin{array}{ll} 1) & y_1^{(j)} \in A_1, y_2^{(j)} \in A_2, \cdots, y_k^{(j)} \in A_k \\ 2) & y_1^{(j)} \in A_{k+1}, y_2^{(j)} \in A_{k+2}, \cdots, y_k^{(j)} \in A_{2k} \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 2^s) & y_1^{(j)} \in A_{k\cdot 2^s-k+1}, \cdots, y_k^{(j)} \in A_{k\cdot 2^s} \end{array}\right\} (1 \leqq j \leqq 2^s)$$

のもとでの解の数の和を考えないといけません．

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)} \quad (1 \leqq j \leqq 2^s)$$

とおくと，方程式 (20) は

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \cdots - y^{(2^s)} = 0 \qquad (21)$$

という簡単な形になります．このとき問題になっているのは，パラメータ m $(0 \leqq m \leqq 2^s - 1)$ の値によって互いに異なっている 2^s 個の条件

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)},$$

$$y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2},\ \cdots,\ y_k^{(j)} \in A_{(m+1)k} \quad (j = 1, 2, \cdots, 2^s)$$

のもとでの方程式 (21) の解の数の和です．

こうして，私たちの結論の最終的な結果を次の命題の形に定式化することができます．

補題 5.　方程式

$$x_1 + x_2 + \cdots + x_l = c, \quad x_i \in A_i,\ 1 \leqq i \leqq l = k \cdot 2^s \qquad (14)$$

の解の数は，$m = 0, 1, \cdots, 2^s - 1$ に対する条件

$$\left.\begin{array}{c} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_k^{(j)}, \\ y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2},\ \cdots,\ y_k^{(j)} \in A_{(m+1)k} \end{array}\right\} (j = 1, 2, \cdots, 2^s)$$

のもとでの方程式

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \cdots - y^{(2^s)} = 0 \qquad (21)$$

の解の数の和を越えない.

明らかに，補題 4 は，補題 5 の $k = s = 1,\ l = 2$ に対応する特殊な場合にあたっています.

さて，準備は完了し，基本補題に取り掛かることができるようになりました.

§5　基本補題の証明

基本補題を，$n-1$ から n への帰納法によって証明しましょう．帰納法の証明をする際，証明すべき主張を強くすると，この方法での論証が根本的にやさしくなることがよくあります (時には，実際そうしてはじめて証明の可能性が生まれることもあるのです)．どうしてそういうことが起こるのかは理解しやすいことです．帰納法での証明では，数 $n-1$ に対して主張が成り立っていることを仮定して，数 n に対して証明するのですが，主張が強いほど，数 $n-1$ の場合に与えられるものが多くなるのです．確かに，数 n に対して証明しなければならないことも多くなるのですが，多くの問題で，$n-1$ での事情の方が n での事情よりも重要なことがあるのです.

今の場合，ちょうどそうなっているのです．方程式 $x_1^n + x_2^n + \cdots + x_k^n = m$ $(1 \leqq m \leqq N)$ の解の数を評価しなければなりません (この際，問題の意味から，ここでは $0 \leqq x_i \leqq m^{\frac{1}{n}} \leqq N^{\frac{1}{n}}$ とします)．しかし，x^n というのは，n 次多項式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

のもっとも簡単な特別の場合で，以下の議論にとっては与えられた方程式 (1) をより一般な方程式

$$f(x_1)+f(x_2)+\cdots f(x_k)=m \tag{22}$$

におき換え，未知数に対してもより広い条件

$$|x_i| \leqq N^{\frac{1}{n}}, \qquad 1 \leqq i \leqq k$$

を課す方が都合が良いのです．方程式 (22) の解の数を評価したとすれば，直接に必要なことよりも多くのことが得られるのです．しかし，証明を見れば分かるでしょうが，まさにこう拡張することによって帰納法の可能性が生まれるのです．それで，$m \leqq N$ に対して，今度は，方程式 (22) の，条件 $|x_i| \leqq N^{\frac{1}{n}}$, $1 \leqq i \leqq k$ を満たす解の数を $r_k(m)$ と書くことにしましょう．この際，帰納法を実現させるために，さらに ($f(x)=x^n$ の場合にも課した条件が満たされている限り) 多項式 $f(x)$ の係数を好きなように扱うことができます．次の主張を証明しましょう．

多項式 $f(x)$ の表示で

$$|a_i| \leqq c(n)N^{\frac{i}{n}} \qquad (0 \leqq i \leqq n) \tag{23}$$

であるとすれば，適当に $k=k(n)$ を選べば

$$r_k(m) < c(n)N^{\frac{k}{n}-1} \qquad (1 \leqq m \leqq N)$$

が成り立つ．

$f(x)=x^n$ の場合，不等式 (23) は，あきらかに，$c(n)=1$ として満たされるので，この主張は確かに基本補題を強くしたものになっています．

まず，$n=1$, $f(x)=a_0x+a_1$ の場合を考えましょう．$k(1)=2$ とおけば，方程式 (22) は

$$a_0(x_1+x_2)=m-2a_1$$

になり，条件 $|x_1| \leqq N$, $|x_2| \leqq N$ を満たすこの方程式の解が問題になりま

す．こうして，x_1 に対する値の可能性は $2N+1 \leqq 3N$ 以下になります．しかし，各 x_1 に対して対応する x_2 は 1 つより多くはないので，

$$r_2(m) \leqq 3N$$

となり，$n=1$ $(k=2)$ に対して主張は証明されました．

今度は $n>1$ として，$n-1$ 次に対して主張が示されているとします．$k(n-1)=k'$ とおき，

$$k = k(n) = 2n \cdot 2^{[4\log_2 k']}$$

と選びます．ここで，2 の肩の指数は $4\log_2 k'$ を越えない最大の整数を表わしています．以下，簡単のために $[4\log_2 k']-1=s$ とおけば，

$$k = 2n \cdot 2^{s+1} \tag{24}$$

となります．

方程式 (22) の解の数 $r_k(m)$ のために，まず，

$$x = \sum_{i=1}^{k/2} f(x_i), \qquad y = \sum_{i=\frac{k}{2}+1}^{k} f(x_i)$$

とおいて，補題 4 を適用します．

集合 A は (今の場合はこれと一致する集合 B も)

$$x = \sum_{i=1}^{k/2} f(x_i), \qquad |x_i| \leqq N^{\frac{1}{n}} \quad \left(1 \leqq i \leqq \frac{k}{2}\right)$$

の形をした和のすべてからなっています．補題 4 の系によって，$r_k(m)$ は，$x \in A,\ y \in A$，つまり

$$x = \sum_{i=1}^{k/2} f(x_i), \qquad y = \sum_{i=1}^{k/2} f(y_i)$$
$$|x_i| \leqq N^{\frac{1}{n}},\ |y_i| \leqq N^{\frac{1}{n}},\ 1 \leqq i \leqq \frac{k}{2}$$

を満たすという条件のもとでの方程式 $x-y=0$ の解の数を越えません．言いかえれば，$r_k(m)$ は，$|x_i| \leqq N^{\frac{1}{n}}$，$|y_i| \leqq N^{\frac{1}{n}}$ $\left(1 \leqq i \leqq \dfrac{k}{2}\right)$ のもとでの方程式

$$\sum_{i=1}^{k/2}\{f(x_i)-f(y_i)\}=0 \tag{25}$$

の解の数を越えません．今度は，$x_i-y_i=h_i$ $\left(1 \leqq i \leqq \dfrac{k}{2}\right)$ とおいて，未知数の系を x_i, y_i から y_i, h_i に替えます．さらに，y_i, h_i $\left(1 \leqq i \leqq \dfrac{k}{2}\right)$ に対して，区間 $[-2N^{\frac{1}{n}},\ +2N^{\frac{1}{n}}]$ のあらゆる整数値を取っても良いとします．そうしても，問題の方程式の解の数は増えるだけですから．こうすると，方程式 (25) の各項 $f(x_i)-f(y_i)$ は

$$\begin{aligned} f(x_i)-f(y_i) &= \sum_{v=0}^{n} a_v\{(y_i+h_i)^{n-v}-y_i^{n-v}\} \\ &= \sum_{v=0}^{n} a_v \sum_{t=1}^{n-v} \binom{n-v}{t} h_i^t y_i^{n-v-t} \end{aligned}$$

という式に変わります．

ここで，和をとる変数を

$$v+t=u$$

とおいて取り替えることにすると，

$$n-v-t=n-u, \quad t=u-v$$

となって，

$$f(y_i+h_i)-f(y_i) = h_i \sum_{v=0}^{n} a_v \sum_{u=v+1}^{n} \binom{n-v}{u-v} h_i^{u-v-1} y_i^{n-u}$$

$$= \ h_i \sum_{u=1}^{n} y_i^{n-u} \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1}$$

$$= \ h_i \sum_{u=1}^{n} a_{i,u} y_i^{n-u} = h_i \varphi_i(y_i)$$

となります[18]．ここで，

$$\varphi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u}$$

は，係数が

$$a_{i,u} = \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1} \quad \left(1 \leqq i \leqq \frac{k}{2}\right)$$

であるような，数 h_i に依存する $n-1$ 次多項式です．

こうして，方程式 (25) は新しい変数 h_i，y_i では

$$h_1\varphi_1(y_1) + h_2\varphi_1(y_2) + \cdots + h_{k/2}\,\varphi_{k/2}\,(y_{k/2}) = 0 \tag{26}$$

という形になります．

この方程式では，数 h_i と y_i は区間 $[-2N^{\frac{1}{n}},\ +2N^{\frac{1}{n}}]$ のどんな整数値を取っても良いのですが，($n-1$ 次の) 多項式 φ_i の係数は数 h_i に依存していることを覚えておかないといけません．

したがって，今の段階で次のことが示されました．

評価の対象である数 $r_k(m)$ は，あらゆる整数値 h_i，$|h_i| \leqq 2N^{1/n}$ $(1 \leqq i \leqq k/2)$ に対する (26) の形のすべての方程式の，整数 y_i，$|y_i| \leqq 2N^{1/n}$ $(1 \leqq i \leqq k/2)$ による解の数の和を越えない．

---

[18] ［訳註］第 2 の等式は (u,v) 平面上の格子点の作るある三角形の異なる表示 $\{(u,v) \in \mathbb{Z}^2 \mid 0 \leqq v \leqq n,\ v+1 \leqq u \leqq n\} = \{(u,v) \in \mathbb{Z}^2 \mid 0 \leqq v \leqq n-1,\ v+1 \leqq u \leqq n\} = \{(u,v) \in \mathbb{Z}^2 \mid 1 \leqq u \leqq n,\ 0 \leqq v \leqq u-1\}$ による．

§6　基本補題の証明：続き

さて，方程式 (26) のうちの 1 つを調べることにしましょう．つまり，当分の間，数 h_i $(1 \leqq i \leqq k/2)$ は固定されていると考えます．この方程式に補題 5 を適用します．この際，未知数 x_i の役をするのは数 $h_i\varphi_i(y_i)$ で，数 l の役をするのは数 $\dfrac{k}{2} = 2n \cdot 2^s$ ですが，簡単のために $2n = k_0$ とおいておきます．ここでもう一度，数 h_i は方程式 (26) の中に，目に見える形で入っているばかりでなく，多項式 φ_i の係数を通しても入っていることを思い出しておきましょう．数 $x_i = h_i\varphi_i(y_i)$ が属さなくてはならない集合 A_i は，今の場合，h_i が与えられた定数値で，数 y_i が区間 $[-2N^{1/n}, +2N^{1/n}]$ を動くときの，$h_i\varphi_i(y_i)$ の形をしたすべての数から成っています．

補題 5 に従えば，方程式 (25) の解で上に述べた条件を満たすものの数は，パラメータ $m = 0, 1, \cdots, 2^s - 1$ の値に対応した 2^s 個の条件

$$\left.\begin{array}{ll} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \cdots + y_{k_0}^{(j)} & \\ y_i^{(j)} \in A_{mk_0+i} & (1 \leqq i \leqq k_0) \end{array}\right\} \quad (1 \leqq j \leqq 2^s)$$

のもとでの，方程式

$$y^{(1)} + y^{(2)} + \cdots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \cdots - y^{(2^s)} = 0 \qquad (21)$$

の解の数の和を越えません．

$m = 0$ の場合 (単に例として選んだだけですが)，方程式 (21) を展開すると，

$$\begin{aligned} \{y_1^{(1)} + y_2^{(1)} + \cdots + y_{k_0}^{(1)}\} + \{y_1^{(2)} + y_2^{(2)} + \cdots + y_{k_0}^{(2)}\} + \cdots \\ \cdots + \{y_1^{(2^{s-1})} + y_2^{(2^{s-1})} + \cdots + y_{k_0}^{(2^{s-1})}\} \\ - \{y_1^{(2^{s-1}+1)} + y_2^{(2^{s-1}+1)} + \cdots + y_{k_0}^{(2^{s-1}+1)}\} - \cdots \\ \cdots - \{y_1^{(2^s)} + y_2^{(2^s)} + \cdots + y_{k_0}^{(2^s)}\} = 0 \end{aligned}$$

という形になり，項を並べ直せば，

$$\left\{y_1^{(1)}+y_1^{(2)}+\cdots+y_1^{(2^{s-1})}-y_1^{(2^{s-1}+1)}-\cdots-y_1^{(2^s)}\right\}$$
$$+\left\{y_2^{(1)}+y_2^{(2)}+\cdots+y_2^{(2^{s-1})}-y_2^{(2^{s-1}+1)}-\cdots-y_2^{(2^s)}\right\}+\cdots$$
$$\cdots+\left\{y_{k_0}^{(1)}+y_{k_0}^{(2)}+\cdots+y_{k_0}^{(2^{s-1})}-y_{k_0}^{(2^{s-1}+1)}-\cdots-y_{k_0}^{(2^s)}\right\}=0$$

となります．ここで，数 $y_i^{(j)}$ はそれぞれ $h_i\varphi_i(v_i^{(j)})$ の形をした数で，$|v_i^{(j)}| \leqq 2N^{1/n}$ を満たすものになっています．それゆえ，この方程式は

$$h_1\left\{\varphi_1(v_1^{(1)})+\varphi_1(v_1^{(2)})+\cdots+\varphi_1(v_1^{(2^{s-1})})\right.$$
$$\left.-\varphi_1(v_1^{(2^{s-1}+1)})-\cdots-\varphi_1(v_1^{(2^s)})\right\}$$
$$+h_2\left\{\varphi_2(v_2^{(1)})+\cdots+\varphi_2(v_2^{(2^{s-1})})-\varphi_2(v_2^{(2^{s-1}+1)})-\cdots-\varphi_2(v_2^{(2^s)})\right\}$$
$$+\cdots\cdots+h_{k_0}\left\{\varphi_{k_0}(v_{k_0}^{(1)})+\cdots\cdots-\varphi_{k_0}(v_{k_0}^{(2^s)})\right\}=0$$

と書き直すことができます．簡単のために，

$$\varphi_i(v_i^{(1)})+\varphi_i(v_i^{(2)})+\cdots+\varphi_i(v_i^{(2^{s-1})})$$
$$-\varphi_i(v_i^{(2^{s-1}+1)})-\cdots-\varphi_i(v_i^{(2^s)})=z_i \qquad (1\leqq i\leqq k_0)$$

とおくと，この方程式はまったく簡単な

$$h_1z_1+h_2z_2+\cdots+h_{k_0}z_{k_0}=0 \tag{27}$$

の形に書き直すことができます．このような型の方程式が全部で 2^s 個ありますが，その全体を簡潔に

$$\sum_{i=1}^{k_0} h_{mk_0+i}z_{mk_0+i}=0 \qquad (0\leqq m\leqq 2^s-1)$$

という形に書くことができます．しかし当分は，方程式 (27) 1 つだけを考えることにしましょう．典型として考えることができるのですから．この方程式の問題としている解の数の評価のためには，まず，$\varphi_i(v_i^{(j)})$ という量が動く範囲がどれ位かを明らかにしないといけません．このために，

$$\varphi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u}$$

$$a_{i,u} = \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1} \quad \left(1 \leqq i \leqq \frac{k}{2}\right)$$

であったことを思い出しておきましょう (§5 (26) 式のすぐ上にあります).

上で $|a_v| < c(n)N^{v/n}$ と $|h_i| < 2N^{1/n}$ という仮定をしているので,

$$|a_{i,u}| < \sum_{v=0}^{u-1} c(n)N^{\frac{v}{n}} \binom{n-v}{u-v} c(n)N^{\frac{u-v-1}{n}} = c(n)N^{\frac{u-1}{n}} \sum_{v=0}^{u-1} \binom{n-v}{u-v}$$

が得られます. つまり, $u \leqq n$ を考慮すれば,

$$|a_{i,u}| < c(n)N^{\frac{u-1}{n}} \tag{28}$$

が得られます. ところで, 一方で $|v_i^{(j)}| \leqq 2N^{\frac{1}{n}}$ でしたから $|v_i^{(j)}|^{n-v} \leqq c(n)N^{\frac{n-u}{n}}$ が得られ, その結果

$$|a_{i,u}| \cdot |v_i^{(j)}|^{n-v} \leqq c(n)N^{\frac{u-1}{n}} N^{\frac{n-u}{n}} = c(n)N^{\frac{n-1}{n}}$$

が得られます. この多項式の項の数は n なので, この評価は $\varphi_i(v_i^{(j)})$ 全体に対しても成り立ちます ($c(n)$ は別のものですが). こうしたわけで,

$$|\varphi_i(v_i^{(j)})| < c(n)N^{\frac{n-1}{n}}, \qquad 1 \leqq i \leqq k_0 \cdot 2^s,\ 1 \leqq j \leqq 2^s$$

が得られます. しかし, z_i は $\pm c(n)N^{\frac{n-1}{n}}$ の形の $2^s = c(n)$ 個の項の和なのですから,

$$|z_i| < c(n)N^{\frac{n-1}{n}}, \qquad 1 \leqq i \leqq 2^s$$

(もちろんこの $c(n)$ は別のものです) が得られます. こうして, 方程式 (27) で, 各 z_i は区間 $\left[-c(n)N^{\frac{n-1}{n}},\ +c(n)N^{\frac{n-1}{n}}\right]$ の中の値しかとることが

できません．

この区間から 1 つの数 m を取りましょう．等式 $z_i = m$ は，一般に言えば，1 通りでなく何通りにも実現可能なのです．数 $v_i^{(j)}$ $(1 \leqq j \leqq 2^s)$ の選び方が異なっても，z_i の値が同じになり得るように，z_i の定義 ((27) 式のすぐ上にあります) がされているのです．そこで，関係式 $z_i = m$ ，つまり，方程式

$$\varphi_i(v_i^{(1)}) + \cdots + \varphi_i(v_i^{(2^{s-1})}) - \varphi_i(v_i^{(2^{s-1}+1)}) - \cdots - \varphi_i(v_i^{(2^s)}) = m \quad (29)$$

の解の数を評価しなければいけませんが，まさにここで帰納法を使うのです．

まず，方程式 (29) を

$$\begin{aligned} &\varphi_i(v_i^{(1)}) + \varphi_i(v_i^{(2)}) + \cdots + \varphi_i(v_i^{(k')}) \\ = \ &m - \varphi_i(v_i^{(k'+1)}) - \cdots - \varphi_i(v_i^{(2^{s-1})}) + \varphi_i(v_i^{(2^{s-1}+1)}) + \cdots + \varphi_i(v_i^{(2^s)}) \end{aligned}$$

の形に書き直します．こうすることが可能なのは，$k' = k(n-1) > 1$ ($k(1) = 2$ であることはすでに分かっています) なので，

$$2^{s-1} = 2^{[4 \log_2 k'] - 2} > k'$$

となるからです[19]．(29) を書き直した方程式の右辺を m' と書けば，

$$\varphi_i(v_i^{(1)}) + \cdots + \varphi_i(v_i^{(k')}) = m' \quad (30)$$

が得られます．数

$$v_i^{(j)} \qquad (k'+1 \leqq j \leqq 2^s)$$

に対して，(もちろん区間 $[-2N^{1/n},\ 2N^{1/n}]$ の中から) 何かある値を選んでおけば，m' は定まった値をもつことになります．帰納法を使いましょう．

---

[19] ［原註］少し詳しく言えば，$k' \geqq 2$，$\log_2 k' \geqq 1$，$3 \log_2 k' \geqq 3$，$[4 \log_2 k'] - 2 > 4 \log_2 k' - 3 \geqq \log_2 k'$，$2^{s-1} = 2^{[4 \log_2 k'] - 2} \geqq k'$ となります．

［訳註］(24) 式前後にある定義により，$k(1) = 2$ から $k(n)$ は帰納的に定まっている．ここにまとめておくと，$k' = k(n-1) \geqq 2$，$s = [4 \log_2 k'] - 1 \geqq 3$，$k = k(n) = 2n \cdot 2^{s+1} > k'$ である．

そのためには必要な条件がすべて満たされていることを確かめなければなりません．さて，

$$\varphi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u}$$

であり，この際 (28) 式によって

$$|a_{i,u}| < c(n) N^{\frac{u-1}{n}} = c(n) \left(N^{\frac{n-1}{n}} \right)^{\frac{u-1}{n-1}}$$

が得られ，また容易に分かるように

$$|m'| < c(n) N^{\frac{n-1}{n}}$$

となっています (なぜなら，m と各 $\varphi_i(y_i^{(j)})$ はこの不等式を満たしているからです)．

この最後の不等式によって，N の役割はここでは $c(n)N^{\frac{n-1}{n}}$ が果たすことができます．すると，多項式 $\varphi_i(y)$ の係数が満たすべき条件 (31) は，条件 (23) で n を $n-1$ にしたものになります．こうして，すべての条件が実際に満たされているのですから，$|v_i^{(j))}| \leqq 2N^{\frac{1}{n}} = 2\left(N^{\frac{n-1}{n}}\right)^{\frac{1}{n-1}}$ に対する方程式 (30) の解の数は，

$$c(n) \left(N^{\frac{n-1}{n}} \right)^{\frac{k'}{n-1}-1} = c(n) N^{\frac{k'-n+1}{n}} \tag{32}$$

を越えません．この評価は，$v_i^{k'+1}, \cdots, v_i^{2^s}$ を固定して得られたものです．あきらかにそのような値の組の数は

$$\left(2N^{\frac{1}{n}} + 1 \right)^{2^s - k'} < c(n) N^{\frac{2^s - k'}{n}} \tag{33}$$

を越えません．それだから，方程式 (29) に対する求める型の解の数は，(32) と (33) の右辺の積を，つまり，

$$c(n)N^{\frac{2^s-n+1}{n}} \tag{34}$$

を越えません.

さて，方程式 (27) に戻りましょう．z_i が区間 $\left[-c(n)N^{\frac{n-1}{n}}, +c(n)N^{\frac{n-1}{n}}\right]$ の中の値しかとることができないことは，すでに示しました ((27) 式の少し下で)．今や，これらの値それぞれの「重複度」(つまり，方程式を満たすような $y_i^{(j)}$ の選び方の数) は，数 (34) を越えません．

この結果から，問題全体を線形方程式の解の数の評価に帰着することができることになります．実際，§5 の終わりで，$r_k(m)$ の評価は，(26) の形の線形方程式の解の数の評価に帰着されています．しかし，$|y_i| \leqq 2N^{1/n}$ を満たす方程式 (26) の解の数は，補題 5 を使って証明したように，2^s 個の (27) の型の方程式，これはすでに線形方程式になっていますが，その解の数の和を越えません．この際，未知数 z_i が動くことのできる範囲も得られています．新しく生まれた困難は (これは線形方程式に移行したために払った代償です)，新しい未知数 z_i がある重複度をもつものと考えなければならないことにあります (これに対しても範囲を定めてあります)．

最後に，これらすべての評価は，数 h_i を選んで固定しているという仮定の上で行われているということを，忘れてはいけません．したがって，これまでに導いた結果に，さらにこのような選び方の総数を掛けなければならないのです．

この節の最終結果をまとめましょう．覚えておいてください．

評価すべき数 $r_k(m)$ は，方程式

$$\sum_{i=1}^{k_0} h_{mk_0+i}\, z_{mk_0+i} = 0 \tag{35}$$

の整数解 z_i で，$|z_i| \leqq c(n)N^{\frac{n-1}{n}}$ を満たし，重複度が $\lambda_i \leqq c(n)N^{\frac{2^s-n+1}{n}}$ をもつものの数の和を越えない．ここで，m は値 $0, 1, \cdots, 2^s-1$ を動き，数 h_r $(1 \leqq r \leqq 2^s k_0)$ は互いに独立に区間 $[-2N^{1/n},\ +2N^{1/n}]$ の中のすべての整数を動く．

こうして，$r_k(m)$ に対して，多項式 $f(x)$ が定式化の中に現れないような評価を得ました．そのため，この評価はまったく一般的な性格をもつのです．

§7　基本補題の証明：終わり

問題が，多項式 $f(x)$ の特定の形によらない線形方程式の解の数の評価に帰着したのですから，補題 3 の助けを借りて，もう簡単に目標に到達できることになります．

数 h_i $\left(|h_i| \leqq 2N^{\frac{1}{n}},\ 1 \leqq i \leqq \dfrac{k}{2}\right)$ の何か特定の組合わせを Γ と書き，この固定した組合わせ Γ とある与えられた m のもとでの方程式 (35) の解の数を $U_m(\Gamma)$ と書きます．この際，解 z_i は不等式 $|z_i| \leqq c(n)N^{\frac{n-1}{n}}$ を満たし，重複度 $\lambda_i \leqq c(n)N^{\frac{2^s-n+1}{n}}$ をもつものを考慮の対象としています．そのとき，前節の最終結果から，

$$r_k(m) \leqq \sum_{\Gamma} \left\{ \sum_{m=0}^{2^s-1} U_m(\Gamma) \right\}$$

となります．ここで和は，数 h_i の許されるあらゆる組合わせ Γ をわたるものです．書きかえれば，

$$r_k(m) \leqq \sum_{m=0}^{2^s-1} \left\{ \sum_{\Gamma} U_m(\Gamma) \right\}$$

となりますが，ただちに明らかなこととして，和 $\displaystyle\sum_{\Gamma} U_m(\Gamma)$ は異なる m に対しても互いになにも違うわけではありません (なぜなら，異なる m に対する方程式 (35) は互いに何も異なっていないからです)．したがって，

$$r_k(m) \leqq 2^s \sum_{\Gamma} U_0(\Gamma) = c(n) \sum_{\Gamma} U_0(\Gamma)$$

と書くことができます．ここで，$U_0(\Gamma)$ は数 h_i $\left(|h_i| \leqq 2N^{\frac{1}{n}},\ 1 \leqq i \leqq \dfrac{k}{2}\right)$

の与えられた組合わせ Γ に対する方程式

$$h_1 z_1 + h_2 z_2 + \cdots + h_{k_0} z_{k_0} = 0 \tag{36}$$

の解の数です．この際，$|z_i| \leqq c(n)N^{\frac{n-1}{n}}$ であり，z_i は重複度 $\lambda_i \leqq c(n)N^{\frac{2^s-n+1}{n}}$ をもっています．すべての z_i の重複度が 1 であるという条件のもとでの，同じ方程式の解の数を $U_0^*(\Gamma)$ と書くなら，明らかに，

$$U_0(\Gamma) \leqq \left\{c(n)N^{\frac{2^s-n+1}{n}}\right\}^{k_0} U_0^*(\Gamma)$$

となります．つまり，$k_0 = 2n$ とおいていたことを思い出すと，

$$U_0(\Gamma) \leqq c(n)N^{2(2^s-n+1)}U_0^*(\Gamma)$$

となり，したがって，

$$r_k(m) \leqq c(n)N^{2(2^s-n+1)} \sum_{\Gamma} U_0^*(\Gamma) \tag{37}$$

となります．

さて，次のことに注意しましょう．各々の Γ は「すべての」h_i $(1 \leqq i \leqq k/2)$ の値の，ある許される組合わせを表わしますが，数 $U_0^*(\Gamma)$ はこれらの値のうち最初の $k_0 = 2n$ 個の値 $(1 \leqq i \leqq 2n)$ で完全に決まってしまいます．というのは，それらだけが方程式 (36) に現れているからです．ある定まった組合わせ Γ を選べば，数 $h_1, h_2, \cdots, h_{2n}$ の値のある組合わせ Γ' が一意的に定まります．しかし逆に，数 $h_1, h_2, \cdots, h_{2n}$ のある組合わせ Γ' を選んだとしても，対応する組合わせ Γ は 1 つではなく，残りの h_i $(2n < i \leqq k/2)$ を好きなように「付け加える」ことができます．各 h_i は区間 $[-2N^{1/n},\ +2N^{1/n}]$ に属さないといけないので，あきらかに，1 つの組合わせ Γ' は

$$c(n)\left(N^{\frac{1}{n}}\right)^{\frac{k}{2}-2n} = c(n)N^{\frac{k}{2n}-2}$$

を越えない数の組合わせ Γ に対応します．したがって，

$$\sum_{\Gamma} U_0^*(\Gamma) \leqq c(n) N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma')$$

となります．ここで，$U_0^*(\Gamma')$ は，数 h_i，$|h_i| \leqq 2N^{1/n}$，$1 \leqq i \leqq 2n$ の組合わせ Γ' を与えたときの，方程式 (36) の整数解 z_i，$|z_i| \leqq c(n)N^{\frac{n-1}{n}}$，$1 \leqq i \leqq 2n$ の解の数であり，和はそのようなすべての組合わせにわたって取られています．したがって，(37) から ($k = 2n \cdot 2^{s+1}$ であることを思い出してください)，

$$\begin{aligned} r_k(m) &\leqq c(n)N^{2(2^s-n+1)} N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma') \\ &= c(n) N^{2(2^{s+1}-n)} \sum_{\Gamma'} U_0^*(\Gamma') \end{aligned} \tag{38}$$

となります．最後に，$\sum_{\Gamma'} U_0^*(\Gamma')$ は，補題 3 によってすぐに評価できます．ただし，$l = 2n$，$A = 2N^{\frac{1}{n}}$，$B = c(n)N^{\frac{n-1}{n}}$ とおかねばなりません．この際，補題 3 のすべての条件が満たされていることは，貴方には容易に確かめることができるでしょう．補題を使えば，

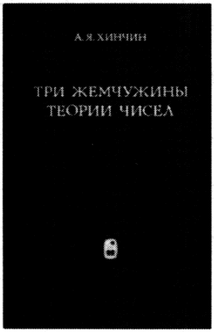
$$\sum_{\Gamma'} U_0^*(\Gamma') \leqq c(n)(AB)^{2n-1} = c(n)N^{2n-1}$$

が得られます．最後に，不等式 (38) から，

$$r_k(m) \leqq c(n)N^{2(2^{s+1}-n)} \cdot N^{2n-1} = c(n)N^{2 \cdot 2^{s+1}-1} = c(n)N^{\frac{k}{n}-1}$$

が得られて，これで基本補題の証明が，と同時にヒルベルトの定理の証明が，完了したことになります．

この証明は，初等的な点で素晴らしいものですが，貴方にはきっと非常に複雑なものに思えるでしょう．しかし，紙と鉛筆を手にして 2-3 週間も頑張れば，完全に理解し会得することができるでしょう．まさに，このような種類の困難を克服することによって，数学者はだんだんと成長していくものなのです．


А. Я. ХИНЧИН
ТРИ ЖЕМЧУЖИНЫ
ТЕОРИИ ЧИСЕЛ

加法的整数論入門

『数論の3つの真珠』の解説として

蟹江幸博

はじめに

この解説は元々ちょっとした附録のつもりで書き始めたものである．しかし附録というのは，言うなら，本の後ろの余白の書き込みのようなもので，フェルマーではないが，すべてを書くには狭すぎる．定義，公理から積み上げていく方が簡潔で正確な記述になるが，厳密さを気にしすぎると，読者そっちのけで細かい議論に熱中することになる．しかも，数学者は概してそれを楽しむ人種である．すると却ってページ数が増す．そこで，ページ数を睨みながら折り合いをつけることになる[1]．記述は教科書風だが，気分は雑談風というスタイルで書いてみた．それでもちょっとした本ほどの厚さになった．

読者としてはもちろん高校生諸君を対象としているが，そうでない人にも読んで欲しいと思っている．考えている読者設定での予備知識は次のようなものである．集合論と代数の初歩については既知とするが，それらは元々ナイーヴな直観を定式化して厳密な議論に耐えるようにしたものなので，使われている記号を見ているうちに自然にわかってくると思う．たとえ知らないためにそのときは分からないことがあっても，あまり気にしないで先に進んで欲しい．

整数についてのやさしい性質には慣れていることにする[2]．偶数，

[1] このためこのような記事で，知識の少ない若い読者と，数学に慣れた読者とを同時に満足させることは至難の業である．この解説では前者に重点をおくことにした．これ以降の脚注は，若い読者のためのものであり，マニア・数学者読むべからずである．

[2] 結局どれくらいの設定なんですかと編集者に訊かれて，「日本人なら子供の頃から風呂で数を数えてますよね．それができればいいんじゃないの」と答えた．しかし，まさかにそんなわけにはいかない．四則演算と集合と文字式の扱いが少しできればいいので，知識レベルとしては中学校 1,2 年くらいあればいい．しかし，指導要領にない項目が許されないというのでは雑談している気がしてこない．ざっとは高校生以上．そして，自分でものを考えるという楽しさを知っている人，または知りたいと思っている人が対象，ということにする．数学的成熟度というような意味不明なものは必要ない．好奇心と集中力はもっていて欲しいが．

一応，後の議論に必要な数の性質は第 1 章 §1 にまとめておいた．そこを読んで上に書いた

奇数，素数，合成数，n 乗数などについてはどんなものかざっとわかっていればよい．必要なことは以下で述べて行く．訳者まえがきに挙げた，完全数や友愛数については多くの本に書いてあるし，以下の議論の流れから離れているので省略する．また，合同数についても G. トス『数学名所案内　上』(1998) の附録 E を参照して貰うことにする．

第 1 章には自然数や整数に関する基礎知識をできるだけコンパクトにまとめてみた．無限にある数のすべてに関して何かを言うためには，どうしても何かが要る．その何かが数学的帰納法の原理である．だから数学の到るところで，さまざまな形で使われている．第 1 章 §2 ではそれをまとめてみた．足し算も掛け算も，じつはこれがないと定義すらできない．割り算はもちろんのことだ．

第 2 章では §1 で，本文の中で証明が読者にゆだねられた，自然数の部分集合の密度についての命題の証明をした．§2 では，自然数の中でも特に興味をもたれる素数について，素数全体の作る部分集合は自然数の中で多いのかそれとも少ないのか，ということに関係した話題のうちで，簡単に証明できることを集めてみた．

第 3 章では，加法的整数論とよばれるもののうち初等的に示すことのできるものをまとめた．自然数を，ある性質をもつ整数[3]の和で表わそうというものである．もちろんいくつ使って表わしてもいいというなら，1 を並べればいいのであって，性質ごとにいくつまで使ってよいかを決めないといけない．そのいくつまでという数をできるだけ少なくするというところに問題の難しさと面白さがある．

ことと違うじゃないかという不満をもつ人もあるだろうが，そのまとめは誰もがもっている数に対する感覚を言葉にしたものにすぎない．分からなくても気にせず，先に進んでもよい．

[3]例えば，素数，n 乗数，n 角数などはそれ自身興味深い対象であり，すべての自然数をそれらの数で表わすことにも強い関心をもちつづけられている．それがゴールドバッハの予想であり，ウェアリングの問題である．n 角数については 19 世紀に解かれてしまったので，問題自身に固有な名前はついていないが，歴史的にはむしろ一番長く懸案となっていたものであろう．これらの問題を解くために作られた概念や条件を少し変えて新しい問題も作られて来た．例えばピュタゴラス数の決定問題は「平方数はいつ 2 つの平方数の和に書けるか」という問題であり，フェルマーの最終定理は「$n \geqq 3$ に対して，n 乗数は 2 つの n 乗数の和に書けない」というものである．

本文の中でいろいろな形で言及される事実の証明が欲しいと思って書き始めた解説だが，事実の中には，今日でも初等的な証明が知られていないものも少なくない．初等的ではあっても，構成が複雑すぎてここには書けないものもある．

事実として昔から知られていても，証明するとなると難しいことも多い．その中で，すべての整数を 3 個の三角数の和で表わす，n 個の n 角数の和で表わす，平方数の和で表わす，n 乗数の和で表わす，2 つの素数の和，3 つの素数の和で表わす，というような問題を扱っている．

また附録として，数の表をつけておいた．おおよそ 10000 までの，素数，平方数 (=四角数)，立方数，4 乗数，三角数，五角数の表である．本文や解説の中で述べられている命題を，表を使って具体的に確かめて欲しい．機械的で詰まらぬことのように思うかもしれないが，やってみれば思いの外に楽しい作業である．

数の表で遊ぶ．なんと人間らしい営みだろう．遊び方のほんの一例を表の前に書いておいた．他の遊び方を見つけた読者は，知らせてほしい．機会があれば紹介したいと思う．

第 1 章

整数の話

この章は，以下の章のための準備の章である．そして§1は，第 1 章のための出発点を指定する，つまり，読者が何を知っていることにするかというためにある．この解説を読みはじめるための予備知識なのだが，じつは終わりの方まで理解できるような人でないと，本当には§1を理解できないかも知れない．

内容的には難しくはないのだが，耳慣れない数学用語が氾濫していて，とても難しく感じる人もいるだろう．分からないと思っても，あまり気にせず，先を読み進んで欲しい．進むのに疲れたと感じたら，時々§1に戻って見て欲しい．すると多分，§1に書いてあることが，戻ってみるたびに，だんだん何でもない当たり前のことに思えてくるはずだ．そして，すべてすでに知っていたと思えるようになったら，本書のどの部分も独力で読みこなすだけの実力が付いていることになる．

ちゃんとした数学の本が読みにくいとすると，多くの場合，本の始めの部分が読みにくいせいだろう．そして，読みやすくしようと思えば，たくさんの説明が必要になり，本当に面白い部分に出くわす前に息切れしてしまうことにもなりかねない．まるで，これから始まる険しい数学山を登るための体力と気力があるかどうかのテストを，本の初めにおくようなものだ．そういう言い方をするなら，ヒンチンの本文はロッククライミングするような難所なのかもしれない．

この解説でも，§1の予備知識を納得するまで書き込めば，数十ページにはなるだろう．それでは書く方も息切れがする．

そこで逆に，できるだけコンパクトにまとめてみた．つらい箇所は，一気

に短時間で通り抜ける，というやり方だ．コンパクトにすれば数学用語が氾濫する．もともとそのために用語を使うのだから．

直接第 3 章が読める読者はそうすればよい．じつはむしろ予備知識をもたない読者の方が，そうした読み方をすべきなのかも知れない．必要な知識なら，たとえば「定理 1.6 により」という形で，記述の中で引用してあるので，その時に初めて定理 1.6 を見ればよい．もちろん，論理的には最初から順に読んで行くように書いてあるが．

多くの人にとって，§1 に書いてあることが本当に理解されていれば，数の知識としてはそれで十分であって，§1 は入り口であると同時にゴールでもある．

§1　数についての予備知識

整数の全体 $\mathbb{Z}$ が以下の性質をもっていることはよく知られている．足し算 $+$ と掛け算 $\times$ (または $\cdot$) という 2 つの演算をもち，それぞれ，結合法則，交換法則，単位元の存在が成り立つ．足し算は加法とも言い，その単位元は 0 であり，任意の元 $a \in \mathbb{Z}$ には逆元 $-a$ が存在する (a の負元と言うこともある)．掛け算は乗法とも言い，その単位元は 1 である．さらに，足し算と掛け算を結ぶものとして，分配法則が成り立つ．これらのことをまとめて，$\mathbb{Z}$ は可換環であると言う．

自然数全体の集合を $\mathbb{N}$ と書く．$\mathbb{N}$ は足し算 $+$ についても掛け算 $\times$ についてもそれぞれ 0 と 1 という単位元をもつ可換半群である．つまり，結合法則と交換法則を満たしているが，逆演算，つまり引き算や割算が自由には行えないということである．

もう 1 つ，重要な注意があった．$0 \neq 1$ ということである．そして，これだけを満たす最小のものが $\mathbb{Z}$ であれば話はすっきりするのだが，そうもいかない．上の条件だけでは，例えば，$1+1$ が何になるか分からない．1 にはなれない．1 になれば，1 の負元を足せば (1 を引くということ) $0=1$ となるから．しかし，$1+1=0$ になることは上の法則の何とも矛盾しない．

困った．しかし，本当に困るのだろうか？　困っていないで，このようなものを位数 2 の**素体** $\mathbb{F}_2$ とよんでしまおう[1]．$\mathbb{F}_2$ は集合としては $\{\underline{\underline{0}}, \underline{\underline{1}}\}$ で，演算は可換で，

$$\underline{\underline{0}} + \underline{\underline{0}} = \underline{\underline{0}} = \underline{\underline{1}} + \underline{\underline{1}},\ \underline{\underline{1}} + \underline{\underline{0}} = \underline{\underline{1}},\ \ \underline{\underline{0}} \cdot \underline{\underline{0}} = \underline{\underline{0}} \cdot \underline{\underline{1}} = \underline{\underline{0}},\ \underline{\underline{1}} \cdot \underline{\underline{1}} = \underline{\underline{1}}$$

であり，$-\underline{\underline{1}}$ と $\underline{\underline{1}}$ は同じものである．$\mathbb{F}_2$ の元 a は 2 倍すると，

$$2 \cdot a = a + a = \underline{\underline{0}}$$

のように，$\underline{\underline{0}}$ になる．ここで，$\underline{\underline{0}}$ と $\underline{\underline{1}}$ は $\mathbb{F}_2$ の元であって，自然数の 0 と 1 とは異なるものだが，2 は自然数である[2]．

0 でない自然数 n を自然数の 1 に掛ければ，$n \cdot 1 = n$ はもちろん 0 でない．しかし，1 が自然数 (整数) でなければ，$n \cdot 1$ が 0 にならないという保証は代数構造の条件からは出てこない．したがって，またこれを仮定しなければならない．出し遅れの証文のように，少しずつ条件を付け加えるのは何だか卑怯な感じがする．そこで，一言で言い切ってみよう．

そのために，記号を 1 つだけ導入する．部分集合 $A \subset \mathbb{Z}$ と 整数 $n \in \mathbb{Z}$ に対し，部分集合 $A + n \subset \mathbb{Z}$ を $A + n = \{a + n \mid a \in A\}$ と定義する．さてこのとき，可換環 $\mathbb{Z}$ と加法半群[3] $\mathbb{N}$ に対する条件は次のことだけしか仮定しない[4]．

---

[1]困ったら名前を付けるというのが，数学者常用の逃げ道である．というより，困った時に，その困ったことをじっと見て，名前を付けられるほどじっと見ていると，たいていの困難は克服されるものである．それでもうまく行かない時は，見方が足らなかったか，多分名前の付け方が悪かったのだろう．

[2]ちょっとした禅問答であるが，楽しむ気になれば，結構楽しいものである．特に若い読者には，楽しんで欲しい．理解しようとするより，楽しもうとして欲しい．きっとそのうち本当に楽しくなる．無味乾燥に見える字句が踊り出す．嘘だと思うなら，確かめてみたらいい．確かめる方法は？　そう，楽しんで読み進むしかない．では禅問答をもう一つ．「一不審（いっぷしん）もって参る．自然数の 2 とはなんぞや？」

[3]乗法半群でもあるが，乗法は加法から，分配法則を満たすように，数学的帰納法を使って一意的に構成される．

[4]もちろん，この条件だけで ($0 \neq 1$ も必要)，$\mathbb{N}$ が一意的に定まるからだが，定義を与えたいわけではないから，気になったとしても今は気にしないように．

「$0 \notin A+1 \subset A \ni 0$ を満たす $\mathbb{Z}$ の部分集合 A は一意的に存在し，$\mathbb{N}$ と同一視できる．」

さて，集合全体として成り立つことをいくつか確認しておこう．$-\mathbb{N} = \{-a \mid a \in \mathbb{N}\}$ と書けば，

$$(\text{A.1}) \qquad \mathbb{Z} = -\mathbb{N} \cup \mathbb{N} \text{ かつ } -\mathbb{N} \cap \mathbb{N} = \{0\}$$

である．また，$x,\ y \in \mathbb{Z}$ には，「$x = y + n$ となる $n \in \mathbb{N}$ が存在する時，$x \geqq y$ または $y \leqq x$ とする[5]」として，演算と両立する全順序 (大小関係) が定義される．つまり，

(1) $a \leqq a \quad (a \in \mathbb{Z})$,　　(2) $a \leqq b,\ b \leqq a\ (a, b \in \mathbb{Z}) \Rightarrow a = b$

(3) $a \leqq b,\ b \leqq c\ (a, b, c \in \mathbb{Z}) \Rightarrow a \leqq c$

(4) 任意の $a, b \in \mathbb{Z}$ に対して，$a \leqq b$ または $b \leqq a$ が成り立つ．

(5) $a \leqq b\ (a, b \in \mathbb{Z}),\ n \in \mathbb{N} \Rightarrow a \pm n \leqq b \pm n,\ na \leqq nb$

が成り立つことが，$\mathbb{N}$ の代数的な性質と上の関係 (A.1) から導かれる[6]．

$\mathbb{N}^{\times} = \mathbb{N} \setminus \{0\} = \mathbb{N} + 1$ は正の整数の集合であり，$(a+1)(b+1) = ab + a + b + 1$ より，積に関して閉じていることが分かる．またこのことから，「$a, b \neq 0 \in \mathbb{Z} \ \Rightarrow\ ab \neq 0$」であることがわかる．その対偶を取れば，「$ab = 0 \in \mathbb{Z} \ \Rightarrow\ a = 0$ または $b = 0$」であること，つまり，$\mathbb{Z}$ が**零因子をもたない**ことが分かる．

---

[5]高校までは 0 は自然数とは考えなかった．代数構造よりも順序構造を基本と考えているからだが，代数構造を基本とする立場では加法の単位元である 0 を含む方が自然である．もちろん (有限) 集合の元の個数を数と考える立場からも 0 がある方が自然である．

そのため，上の定義をそのままに，$\mathbb{N}$ が 0 を含まない立場をとれば，定義されるのは「$x > y$」であり「$y < x$」である．そして，$x \geqq y$ は $x > y$ または $x = y$ のときと定義することになる．

今は，$x \geqq y$ かつ $x \neq y$ のとき $x > y$ とするのである．どちらが正しいかということではなく，$\leqq$ と $<$ のどちらを基本的な関係と思うか，ひいては 0 を自然 (数) と思うか否かという立場の違いによるものなのである．不等式の記号自身もじつは，$\geqq$ よりも $\geq$ を使うことが多いのだが，高校生向けのシリーズであることも考えて，記号は $\geqq$ を採用した．

[6]証明は読者の楽しみに残しておく．

§2 数学的帰納法

上の条件から，自然数の集合 $\mathbb{N}$ の性質として

$$(\text{MI0}) \qquad 0 \in A \subset \mathbb{N},\ A+1 \subset A \ \Rightarrow A = \mathbb{N}$$

を抽出すると，$\mathbb{N}$ は，$\mathbb{Z}$ の部分加法半群であることと，$0 \notin \mathbb{N}+1$ とこの (MI0) だけで一意的に定まるほど，この性質は重要である[7].

(MI0) は，数学的帰納法 (Mathematical Induction) として知られる論証法の集合論版になっている．$P(n)$ を自然数 n に関する命題とする．

定理 1.1 (数学的帰納法 MI1). 「$P(0)$ が真」かつ「$P(m)$ が真 $(m \in \mathbb{N}) \Rightarrow P(m+1)$ が真」が成り立てば，すべての $n \in \mathbb{N}$ に対して $P(n)$ が真である．

この 2 つが同値であることは，$A = \{n \in \mathbb{N} \mid P(n)\text{ が真}\}$ とおけば，すぐに分かる．

初期点を変えることによって，(MI1) は次のように変形される．

定理 1.2 (数学的帰納法 MI1′). $a \in \mathbb{Z}$ とする．「$P(a)$ が真」かつ「$P(m)$ が真 $(m \geqq a) \Rightarrow P(m+1)$ が真」が成り立てば，すべての $n \geqq a$ に対して「$P(n)$ が真」である．

(MI1′) はその集合論版

$$(\text{MI0}') \qquad a \in A \subset \mathbb{Z},\ A+1 \subset A \ \Rightarrow A \supset \{x \in \mathbb{Z} \mid x \geqq a\}$$

が (MI0) の変形として，$B = A - a = \{b - a \mid b \in B\}$ とおくことで得ら

---

[7] じつは，部分加法半群であるという仮定も必要ではなく，その代わりに「$a \neq b (\in \mathbb{N}) \Rightarrow a+1 \neq b+1$」という性質を満たす「$+1$」という操作があるだけで良いのだが，それは少し難しい．

れることから，ただちに得られる．以降の (MI) の変化形でも，初期値を移動させることができる．また応用上は，a に色々な値を使うことができるこの形で用いられることが多い．

例 1. すべての $n \in \mathbb{N}^{\times}$ に対し，命題 $P(n)$:「$1+2+\cdots+n=n(n+1)/2$」が成り立つことを数学的帰納法で示す．

$P(1): 1=1$ は真．$P(m)$ が真だとすれば，$P(m+1)$ の左辺は，

$$1+2+\cdots+m+(m+1)=\frac{m(m+1)}{2}+(m+1)=\frac{(m+1)(m+2)}{2}$$

となって，$P(m+1)$ も真．

数学的帰納法の変化形には，

定理 1.3 (数学的帰納法 MI2). **「$P(0)$ が真」かつ「$m \in \mathbb{N}$ に対し，$P(k)$ が真 $(0 \leqq k \leqq m) \Rightarrow P(m+1)$ が真」が成り立てば，すべての $n \in \mathbb{N}$ に対して「$P(n)$ が真」である．**

もある．(MI1) より示すべき条件が弱いので「(MI2) $\Rightarrow$ (MI1)」だが,「(MI1) $\Rightarrow$ (MI2)」も示すことができる[8]．また，(MI1) と (MI2) との中間形

定理 1.4 (数学的帰納法 MI1.5). **$l \in \mathbb{N}$ を取る.「$P(0), \cdots, P(l)$ が真」かつ「$m \in \mathbb{N}$ に対し，$P(k)$ が真 $(m-l \leqq k \leqq m) \Rightarrow P(m+1)$ が真」が成り立てば，すべての $n \in \mathbb{N}$ に対して「$P(n)$ が真」である．**

もよく使われる形である ($l=1,2$ で使われることが多い)．

自然数全体に対する性質を示すのには，本質的には数学的帰納法を使う以外の方法はない．しかし，ある特定の自然数 (1 であることが多い) に対する命題も，(MI) の変化形を使って示すことができることがある．言い換えの基礎となる次の定理はそれ自身重要である．

---

[8] これには，有限帰納法が任意有限個の対象について成立することが必要である．当たり前だと思うのならそれでも良い．証明が気になるのなら，考えてみること．

定理 1.5. $\emptyset \neq A \subset \mathbb{N} \Rightarrow A$ **に最小元がある**[9]**.**

証明. A の $\mathbb{N}$ での下界の集合 $B = \{n \in \mathbb{N} \mid n \leqq a\ (\text{すべての}\ a \in A)\}$ を考えると，$0 \in B$ は明らか.

どんな $m \in \mathbb{N}$ に対しても「$m \in B \Longrightarrow m+1 \in B$」ならば，(MI0) により $B = \mathbb{N}$ となるが，$A \neq \emptyset$ に反するので，これは起こらない．ある $m \in \mathbb{N}$ に対して「$m \in B$ かつ $m+1 \notin B$」とすると，$m \in A$ が A の最小元となる. □

無限降下法はフェルマーが編み出したもので，フェルマーの驚くべき発見の証明はこれによってなされていることが多い[10].

定理 1.6 (無限降下法 MI3). **「ある** $k \in \mathbb{N}^{\times}$ **に対して** $P(k)$ **が真」かつ「**$k > 1$ **ならば，ある** $0 < k' < k$ **があって** $P(k')$ **が真」が成り立てば，「**$P(1)$ **が真」である.**

証明. $A = \{n \in \mathbb{N}^{\times} \mid P(n)\ \text{が真}\}$ とおくと，最初の仮定から $k \in A$ であり $A \neq \emptyset$ である．したがって，A には最小元 a がある．$a = 1$ なら証明は終る．$a > 1$ なら，仮定により，$0 < n < a$ があって，$P(n)$ は真．ゆえに，$n \in A$ だが，これは a の最小性に矛盾する. □

また，空でない部分集合に最小元があるという上の事実の重要性を示すものとして，整数の割算の可能性が示される.

定理 1.7 (整数の割り算). $a, b \in \mathbb{Z},\ b > 0$ **に対して，**

$$a = qb + r, \quad q, r \in \mathbb{Z},\ 0 \leqq r \leqq b - 1$$

を満たす q, r **が一意的に存在する.**

---

[9] この定理を「$\mathbb{N}$ の空でない部分集合は最小元をもつ」と一息で言い切ってみると，記憶のためにも理解のためにも役に立つ.

[10] 以下の章で例を見ることになる．命題を見れば「無限降下」でなくて,「有限降下」ではないかという人もいるかも知れない．しかし,「任意有限」というのは「限り」が「無い」.

証明.　$\mathbb{Z}$ の部分集合 $a+b\mathbb{Z}=\{a+bx \mid x\in\mathbb{Z}\}$ と $\mathbb{N}$ の共通部分である $\mathbb{N}$ の部分集合の最小元を r とする．$r \geqq b$ であれば，$r-b\in(a+b\mathbb{Z})\cap\mathbb{N}$ となるが，これは r の最小性に矛盾する． □

§3　約数・倍数とイデアル

$a=bc$ を満たす $a,b,c\in\mathbb{N}$ に対して，b と c を a の**約数**と言い，a を b と c の**倍数**と言う．このとき，b は a **を割る**とも言い，$b|a$ と書く．a の約数の全体を $D(a)$ と書こう．

整数に対しても約数，倍数を同様に定義する．$a\in\mathbb{N}\subset\mathbb{Z}$ であるが，自然数 a の約数と言うときは自然数だけ，整数 a の約数と言うときは整数だけ考える．a の約数の全体を $\mathcal{D}(a)$ または $D(a)$ と書こう:

$$\mathcal{D}(a)=\{b\in\mathbb{Z}\mid b|a\}\subset\mathbb{Z},\quad D(a)=\mathcal{D}(a)\cap\mathbb{N}.$$

例えば，自然数 6 の約数は 1,2,3,6 であり，整数 6 の約数は $\pm1,\pm2,\pm3,\pm6$ である．つまり，$D(6)=\{1,2,3,6\}$, $\mathcal{D}(6)=\{\pm1,\pm2,\pm3,\pm6\}$ である[11]．

倍数についても記号を用意しよう．$a\in\mathbb{Z}$ または $a\in\mathbb{N}$ の倍数の全体を

$$\mathcal{I}(a)=a\mathbb{Z}=\{az\mid z\in\mathbb{Z}\}=\{z\in\mathbb{Z}\mid a|z\},$$
$$I(a)=a\mathbb{N}=\{an\mid n\in\mathbb{N}\}=\{n\in\mathbb{N}\mid a|n\}$$

と書こう[12]．すると，明らかに $\mathcal{I}=\mathcal{I}(a)$ は

$$\mathcal{I}+\mathcal{I}=\{a+b\mid a,b\in\mathcal{I}\}\subset\mathcal{I},\quad x\mathcal{I}\subset\mathcal{I}\ (x\in\mathbb{Z})$$

を満たす．この 2 つの性質を満たす $\mathbb{Z}$ の部分集合 $\mathcal{I}$ を**イデアル**と言う．また，$\mathcal{I}(a)$ のように 1 つの数から生成された[13]イデアルを**主イデアル**と言う．

---

[11]($\mathbb{Z}$ は零因子をもたないので) どんな $a(\neq 0)\in\mathbb{Z}$ に対しても $\mathcal{D}(a)$ は 0 を含まない有限集合になり，また $\mathcal{D}(0)=\mathbb{Z}$ となる．

[12]どんな $a(\neq 0)\in\mathbb{Z}$ に対しても $\mathcal{I}(a)$ は 0 を含む無限集合になり，また $\mathcal{I}(0)=\{0\}$ となる．

[13]この場合，生成されたというのは a を含むイデアルで最小のものという意味．2 つの元 a,b

$\mathcal{I}, \mathcal{I}' \subset \mathbb{Z}$ がイデアルであれば，$\mathcal{I} \cap \mathcal{I}'$ と $\mathcal{I} + \mathcal{I}' = \{a + b \mid a \in \mathcal{I}, b \in \mathcal{I}'\}$ もまたイデアルである．これを示すのは容易である．$\mathbb{Z}$ の次の性質は重要である．

定理 1.8. **整数環 $\mathbb{Z}$ は主イデアル整域** (つまり，すべてのイデアルが主イデアルであるような整域) **である．**

証明. 整域とは，$0 \neq 1$ であって零因子をもたない可換環のことだから，すでに示されている．

さて，$\mathcal{I} \subset \mathbb{Z}$ を $\{0\}$ でないイデアルとする．$\mathcal{I} \cap \mathbb{N}^{\times} \subset \mathbb{N}$ の最小元を a と書く．$\mathcal{I} \supset a\mathbb{Z}$ であるが，$\mathcal{I} = a\mathbb{Z}$ なら証明は終っている．そこで $\mathcal{I} \neq a\mathbb{Z}$ と仮定する．すると，$b \in \mathcal{I} \setminus a\mathbb{Z}$ となる元があるが，$b \neq 0$ である．必要ならば -1 を掛けて，$b > 0$ としてよい．そこで，a による整数としての割算をする．

$$b = qa + r, \quad q, r \in \mathbb{N},\ 0 \leqq r < a$$

を満たす r は $\mathcal{I}$ の元となるが $(r = qa - b)$，$b \notin a\mathbb{Z}$ であれば $r > 0$ であり，a の最小性に矛盾する． □

注意 1.9. 証明から明らかだが，イデアルの生成元は符号を除いて一意的であり，正の生成元は 1 つしかない．その上，イデアルの任意の元は生成元の倍数になっている．

自然数 $a,\ b$ に対して，$\mathcal{D}(a) \cap \mathcal{D}(b)$ ないし $D(a) \cap D(b)$ の元を $a,\ b$ の**公約数**と言う．$D(a) \cap D(b)$ は有限集合だから最大元がある．それを**最大公約数**と言い，(a, b) または $\gcd(a, b)$ と書く[14]．

定理 1.10. $a,\ b \in \mathbb{N}$ **に対して次が成り立つ．**

1. $b | a \iff (a, b) = b$ **．**

なら，生成されたイデアルは $\mathcal{I}(a, b)$ と書かれるが，じつは $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$ である．

[14]greatest common divisor.

2. $D(a) \cap D(b) = D((a,b))$, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}((a,\ b))$.

3. (a,b) **はイデアル** $\mathcal{I}(a,b) = a\mathbb{Z} + b\mathbb{Z}$ **の正の生成元である.**

自然数 $a,\ b$ に対して，$\mathcal{I}(a) \cap \mathcal{I}(b)$ の元を $a,\ b$ の**公倍数**と言う．$\mathcal{I}(a) \cap \mathcal{I}(b) \cap \mathbb{N}^{\times}$ の最小元を**最小公倍数**と言い，$\mathrm{lcm}(a,b)$ と書く[15].

定理 1.11. $a,\ b \in \mathbb{N}$ **に対して，**

1. $b|a \iff \mathbf{lcm}(a,b) = a$.

2. $\mathcal{I}(a) \cap \mathcal{I}(b) = \mathcal{I}(\mathbf{lcm}(a,b))$.

3. $\mathbf{lcm}(a,b)$ **はイデアル** $\mathcal{I}(a) \cap \mathcal{I}(b)$ **の正である元の最小のもので，生成元である.**

定理 1.10 と 1.11 は双対的な定理である．定理 1.11 だけを簡単に示そう．主張の 1. は明らかである．3. の証明をする．

簡単のために，$d = (a,b)$ と書く．$\mathcal{I}(a,b)$ の生成元 δ は上の注意 1.9 により，a,b の公約数であるので，$\delta \leqq d$ であることがわかる．また a,b の公約数は，したがって d は すべての $\mathcal{I}(a,b) = a\mathbb{Z} + b\mathbb{Z}$ の元の約数になるので，$d \leqq \delta$ でもある．こうして，$d = \delta$ であることが分かる．3. は示された．3. から 2. はただちに分かる． □

定理 1.10 の応用としてよく使われる補題がある．

補題 1.12. $(a,b) = 1,\ a|bc \implies a|c$.

証明. 定理 1.10 の 3. を (a,b) の場合に使うと，$\mathcal{I}(a,b) = \mathbb{Z}$ だから，$ma + nb = 1$ を満たす $m,n \in \mathbb{Z}$ がある．また，$a|bc$ より $bc = ak$ を満たす $k \in \mathbb{Z}$ がある．したがって，$nak = nbc = (1 - ma)c$ となり，移項すれば $c = a(nk + mc)$ となる． □

---

[15] least common multiple.

§4　素因数分解の一意性

0 以外の自然数 n は，その約数の個数が 1 個のとき**単数** (1 のみ)，2 個のとき**素数**，3 個以上のとき**合成数**とよばれる．n が合成数なら，$n = ab$, $1 < a, b < n$ と書かれるので，(数学的帰納法により) 素数の積に分解する．さらに，前節の補題を使って，数学的帰納法を使えば,「算術の基本定理」ともよばれる次の定理が得られる．

定理 1.13 (素因数分解の一意性).　**任意の自然数 $n > 1$ は素数の積に，順序を除いて一意的に分解される．つまり，n に対して，一意的に素数 $p_1 < \cdots < p_k$ と指数 $e_1, \cdots, e_k$ $(e_i > 0)$ が存在して，**

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

と書かれる．

証明.　n が素数なら良い．素数でなければ合成数で，$n = a \cdot b$, $0 < a \leqq b < n$ と書かれる．帰納法を使えば素因数の積に分解できることはすぐに分かる．

別の素因数分解 $n = q_1^{f_1} \cdots q_h^{f_h}$, $q_1 < \cdots < q_h$ があったとしよう．異なる分解であるなら，ある $g \geqq 1$ があって，$p_i = q_i$ かつ $e_i = f_i (1 \leqq i \leqq g - 1)$ であって，1) $p_g < q_g$ であるか，2) $p_g = q_g$, $e_g < f_g$ であるとしてよい．

1) の時は $p_1^{e_1} \cdots p_{g-1}^{e_{g-1}}$ で n を割ることによって，2) の時は $p_1^{e_1} \cdots p_g^{e_g}$ で n を割り，素因数の記号を変えることによって，最初から $p_1 < q_1$ と仮定することができる．

素数同士は，異なれば互いに素であるから，§2 の補題によって，p_1 は q_j の約数にならなければならないが，q_j はすべて p_1 より大きい素数だから，そういうことは起こらない．　□

素因数分解の一意性から，$n = p_1^{e_1} \cdots p_k^{e_k}$ の約数の集合と，n の約数の数が

$$D(p_1^{e_1}\cdots p_k^{e_k}) = \{p_1^{f_1}\cdots p_k^{f_k} \mid 0 \leqq f_i \leqq e_i\ (1 \leqq i \leqq k)\},$$
$$|D(p_1^{e_1}\cdots p_k^{e_k})| = \prod_{i=1}^{k}(1+e_i)$$

であることが分かる[16].

a,b の最大公約数や最小公倍数も素因数分解を使って表わすことができる.指数に 0 であることも許すことによって，共通の素因数を使って

$$a = p_1^{e_1}\cdots p_k^{e_k},\quad b = p_1^{f_1}\cdots p_k^{f_k}\quad (0 \leqq e_i,\ f_i)$$

と表わす. (表示を一意的にしたければ $e_i + f_i > 0$ という条件を付ければよい.)　そのとき，$g_i = \min(e_i,\ f_i)$, $h_i = \max(e_i,\ f_i)$ とおけば，$g_i + h_i = e_i + f_i$ であり

$$\gcd(a,b) = p_1^{g_1}\cdots p_k^{g_k},\quad \mathrm{lcm}(a,b) = p_1^{h_1}\cdots p_k^{h_k},$$
$$\gcd(a,b)\cdot\mathrm{lcm}(a,b) = ab = p_1^{g_1+h_1}\cdots p_k^{g_k+h_k}$$

となる.

$(a,b)=1$ である $a,b\in\mathbb{N}$ を**互いに素**であるというのは，a,b の素因数分解の際，共通の素因数が存在しないことによる.

また以下で使う便宜のために，定理 1.13 によって簡単に得られる素数の特徴づけをまとめておく.

定理 1.14 (素数の特徴づけ).　**正の整数 p に関して，次の命題は同値である.**

1. p **は素数である.**

2. p **は** a $(1 \leqq a \leqq p-1)$ **と互いに素である.**

3. p **と** $(p-1)!$ **は互いに素である.**

4. $p|ab,\ a,b\in\mathbb{N}$ **ならば,** $p|a$ **または** $p|b$ **である.**

---

[16] 有限集合 A の元の個数を A の位数と言い，$|A|$ または $\#A$ と表わすこと，積 $a_1a_2\cdots a_k$ を $\prod_{i=1}^{k} a_i$ という記法で表わす.

§4.1 $n!$ の素因数分解

第 2 章 §2.5 で使うので，$n!$ の素因数分解 $n! = p_1^{e_1} \cdots p_k^{e_k}$ を具体的に考えてみる．n 以下の素数すべてがこの分解に出てくる．素数 $p \leqq n$ の $n!$ の素因数分解における指数 e を与えるのが次の定理である．

定理 1.15 (ルジャンドル).

$$e = \sum_{l \geqq 1} \left[\frac{n}{p^l} \right] .$$

証明. $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$ の因数のうち p の倍数は $\left[\frac{n}{p} \right]$ 個ある．p^2 の倍数も $\left[\frac{n}{p^2} \right]$ 個あり，本来これに対して p のベキ 2 つ分と数えるべきだが，すでに p の倍数としても数えられているので，p のベキ 1 つ分をつけ加えると考える．$l \geqq 3$ に対する p^l の倍数でも同様である．あとは $p^l > n$ となる l に対して $\left[\frac{n}{p^l} \right] = 0$ であることに注意する． □

§5 合同式と合同類

自然数 $n \in \mathbb{N}$ に対して，差が n の倍数である 2 つの整数 $a, b \in \mathbb{Z}$ を **n を法として合同**であると言い，$a \equiv b \pmod{n}$ と書く．合同に関して簡単に分かることをまとめておこう．

定理 1.16. $n \in \mathbb{N}$ に対して，以下の命題が成り立つ．

1. $a \equiv 0 \pmod{n} \iff n|a \iff a = nb$ となる $b \in \mathbb{Z}$ がある．

2. **1.** $a \equiv a \pmod{n}$ (反射律)

2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (対称律)

3. $a \equiv b, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (推移律)

3. $a \equiv b,\ c \equiv d \pmod{n} \Rightarrow a \pm c \equiv b \pm d,\ ac \equiv bd \pmod{n}$ **.**

4. $(a,n)=1$ **とすると，**$ab \equiv 1 \pmod{n}$ **となる数** $b \in \mathbb{Z}$ **が存在する．さらに，**

1. $ab \equiv 0 \pmod{n} \Rightarrow b \equiv 0 \pmod{n}$

2. $ab \equiv ac \pmod{n} \Rightarrow b \equiv c \pmod{n}$

が成り立つ．

4. 以外の証明はやさしく，4. の証明は §2 の最後の補題 1.12 とその証明からすぐ分かる．

a と n を法として合同な整数の全体は $a+n\mathbb{Z}$ であり，a の (n を法とした) **合同類**と言い，$[a]_n$ または $[a]$ と書く．異なる合同類が n 個しかないことは，整数としての n による割り算の余りが $R_n = \{0,1,\cdots,n-1\}$ の n 通りしかないことから分かる．そこで，各合同類を 1 つの元と考える，n 個の元からなる集合 $\mathbb{Z}_n$ を考えると，定理の 3. によって可換環の構造が入る[17]．加法の単位元は $[0]=n\mathbb{Z}$ であり，乗法の単位元は $[1]=1+n\mathbb{Z}$ である．R_n のように各合同類から 1 つずつ数を選んで得られる n 個の数の集合を $\mathbb{Z}_n$ の**代表系**と言う．

n が合成数であれば，$n=ab$ となる $a,b \in R_n$ がある，つまり，零因子をもつので，$\mathbb{Z}_n$ は整域ではない．

では，$[a]$ が $\mathbb{Z}_n$ の零因子にならないのはどういうときだろうか．逆に零因子になる条件を見てみよう．$[a]$ が零因子であるとは，$[b] \neq [0]$ があって $[a][b]=[ab]=[0]$ であるということで，合同式で書けば $ab \equiv 0 \pmod{n}$ となる．つまり，$ab \in n\mathbb{Z}$ となる $b \notin n\mathbb{Z}$ が存在するような $a \notin n\mathbb{Z}$ を代表元とするということである．

$d=(a,n)$ が 1 かどうかによって，$[a]$ が零因子かどうかが分かれる．実際，$d>1$ であれば，$a=cd,\ n=md\ (m<n)$ となる．すると $am = cdm = cn \in n\mathbb{Z}$ となる．$d=1$ であれば，$ab=nk$ から $n|b$ が従う．

さらに $(a,n)=(a \pm n, n)$ から，この条件は代表元の取り方によらない

[17]これを一言で言うと，可換環 $\mathbb{Z}$ のイデアル $n\mathbb{Z}$ による**剰余環**という．$[a] \pm [b] = [a \pm b]$，$[a]\cdot[b]=[ab]$ と定義しても矛盾しない保証が 3. だと言っているのである．

ことがわかる．

零因子にならない合同類を**既約合同類**と言い，既約合同類の作る部分集合を $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ と書く．$\mathbb{Z}_n^\times$ の元の個数を $\varphi(n)$ と書き，**オイラーの関数**と言う．また，すべての既約合同類から 1 つずつ数を選んだ，$\varphi(n)$ 個の数の集合を**既約代表系**と言う．$P_n = \{a \mid 1 \leqq a \leqq n,\ (a,n) = 1\}$ は 1 つの既約代表系になっている．あきらかに $1 \in P_n$ である．このとき，

定理 1.17.　既約合同類の集合 $\mathbb{Z}_n^\times$ は乗法群である．

証明.　定理 1.13 から容易に得られる次の補題によって，$\mathbb{Z}$ に定義された積に関して $\mathbb{Z}_n^\times$ が閉じていることが分かる．

補題 1.18.　$(a,n) = (b,n) = 1 \Longrightarrow (ab,n) = 1$.

逆元の存在を示そう．既約代表系 P_n と，数 $a \in P_n$ をとろう．$aP_n = \{ab \mid b \in P_n\}$ の各元が n を法として互いに合同でないことを示そう．

もし $ab \equiv ac \pmod{n}$ とすると，$(a,n) = 1$ であるから，定理 1.16 の 4. から，$b \equiv c \pmod{n}$ となる．

aP_n の元の数も $\varphi(n)$ であることから，aP_n も既約代表系であることがわかる．したがってこの中のある元 ab が 1 と合同でなければならない．□

p が素数なら，$P_p = \{0, 1, 2, \cdots, p-1\}$, $\varphi(p) = p - 1$ であり，$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]\}$ である．$\mathbb{Z}_p^\times$ が乗法群になるので，$\mathbb{Z}_p$ は体である．

また $n = 1$ のときは，$R_1 = \{0\}$, $P_1 = \{1\}, \varphi(1) = 1$ となる．

例としていくつかの $\mathbb{Z}_n$ での加法と乗法の表を挙げてみる．

$\mathbb{Z}_2$ で，

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$ で，

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_6$ で，

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}_6^\times$ で，

$\times$	1	5
1	1	5
5	5	1

§6　オイラーの関数の性質

オイラーの関数 $\varphi(n)$ の性質をまとめておく．

定理 1.19.

1. $(m,n)=1$ **ならば，** $\varphi(mn)=\varphi(m)\varphi(n)$**.**

2. p **が素数なら，** $\varphi(p^e)=p^e-p^{e-1}=p^e\left(1-\dfrac{1}{p}\right)$ **である．**

3. n **の素因数を** $p_1,\cdots,p_k$ **とすると，** $\varphi(n)=n\displaystyle\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$ **である．**

4. $\displaystyle\sum_{d|n}\varphi(d)=n$**.**

証明.　2. を先に示す．p が素数だから「$(a,p^e)>1 \Leftrightarrow p|a$」であり，$R_{p^e}$ の中の p の倍数は p^{e-1} 個ある．

1. は群論を使って，$\mathbb{Z}_m^\times\times\mathbb{Z}_n^\times\cong\mathbb{Z}_{mn}^\times$ を示すことが多いが，元の数だけなら，$\mathbb{Z}_m^\times$ と $\mathbb{Z}_n^\times$ の既約代表系をそれぞれ，$\{a_i \mid 1\leqq i\leqq\varphi(m)\}$ と $\{b_j \mid 1\leqq j\leqq\varphi(n)\}$ とするとき $\{na_i+mb_j \mid 1\leqq i\leqq\varphi(m),\ 1\leqq j\leqq\varphi(n)\}$ が $\mathbb{Z}_m^\times\times\mathbb{Z}_n^\times\cong\mathbb{Z}_{mn}^\times$ の既約代表系であることを示せばよい．

1. と 2. が示されれば，3. はただちに得られるが，ここでは，3. を直接証明することにする．3. から 1. は明らかである．

3. の証明.　右辺を展開すると

$$
\begin{aligned}
n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) &= n-\sum_{i=1}^{k}\frac{n}{p_i}+\sum_{i<j}\frac{n}{p_ip_j}-\cdots \\
&\quad \cdots+(-1)^k\sum_{i_1<i_2<\cdots<i_k}\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}
\end{aligned}
$$

となる．一般項の $\dfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}}$ は $\{m \mid 1 \leqq m \leqq n,\ p_{i_1}p_{i_2}\cdots p_{i_r}|m\}$ の元 (数) の個数だから，$l(m)$ を $\{i \mid p_i|m\}$ の元の数とおくと，

$$
\sum_{i_1<i_2<\cdots<i_r}\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}}=\sum_{m=1}^{n}\sum_{i_1<i_2<\cdots<i_r,\ p_{i_1}p_{i_2}\cdots p_{i_r}|m}1=\sum_{m=1}^{n}\begin{pmatrix} l(m) \\ r \end{pmatrix}
$$

となるから，

$$
\begin{aligned}
n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) &= \sum_{m=1}^{n}\sum_{r=0}^{l(m)}(-1)^r\begin{pmatrix} l(m) \\ r \end{pmatrix} \\
&= \sum_{m,\ l(m)>0}(1-1)^{l(m)}+\sum_{m,\ l(m)=0}1=\varphi(n)
\end{aligned}
$$

となる．最後の等式は,「$l(m)>0 \Leftrightarrow (m,n)>1$」に注意すればよい．

4. の証明.　3. により，$n=p^e$ のときは (p は素数),

$$
\sum_{d|n}\varphi(d)=\sum_{i=0}^{e}\varphi(p^i)=1+\sum_{i=1}^{e}(p^i-p^{i-1})=p^e
$$

となる．したがって，$n=p_1^{e_1}\cdots p_k^{e_k}$ であれば，$D(n)$ の構造と 1. から，

$$
\sum_{d|n}\varphi(d) = \sum_{i=1}^{k}\sum_{f_i=0}^{e_i}\varphi(p_1^{f_1}\cdots p_k^{f_k})=\sum_{i=1}^{k}\sum_{f_i=0}^{e_i}\varphi(p_1^{f_1})\cdots\varphi(p_k^{f_k})
$$

$$= \prod_{i=1}^{k} \left(\sum_{f_i=0}^{e_i} \varphi(p_i^{f_i}) \right) = \prod_{i=1}^{k} p_i^{e_i} = n$$

となる[18]. □

§7 素数あれこれ

素数がどれくらいあるかというような話題は第 2 章ですることにして，ここでは素数に関連したいくつかの結果を述べておく.

§7.1 オイラーの定理とフェルマーの小定理

定理 1.20 (オイラー). $(a, n) = 1$ **ならば，** $a^{\varphi(n)} \equiv 1 \pmod{n}$ **である.**

証明. $\mathbb{Z}_n^\times$ が乗法群であることを示す定理 1.17 の証明から，P_n も aP_n も既約代表系なので

$$\prod_{b \in P_n} b \equiv \prod_{c \in aP_n} c = \prod_{b \in P_n} ab = a^{\varphi(n)} \prod_{b \in P_n} b \pmod{n}$$

である．定義により $(\prod_{b \in P_n} b, n) = 1$ であるから，

$$1 \equiv a^{\varphi(n)} \pmod{n}$$

となる. □

定理 1.20 で n を素数 p とすれば，系として，フェルマーの小定理として知られる次の定理が得られる.

系 1.21 (フェルマー). $p \nmid a$ **なら** $a^{p-1} \equiv 1 \pmod{p}$ **である.**

[18] 4. がオイラーの関数を特徴付けていることも分かるが，ここでは示さない.

この定理は数論での多くの応用をもっているが，最近公開鍵暗号の基本原理としても有名になった．

§7.2 ウィルソンの定理

定理 1.22 (ウィルソン). p : **素数** $\Longleftrightarrow (p-1)! \equiv -1 \pmod p$

いくつか証明があるが，ガウスによる初等的な証明を紹介しておく．

証明. $\Longrightarrow$) $p=2$ のときは明らかだから，p を奇素数とする．

数 $a \in P_p$ は mod$p$ での逆元 $a' \in P_p$ をもつ．$a = a'$ となるのは 1 と $p-1$ だけである．というのは，$1 = aa' \equiv a^2 \pmod p$ であり，$(a-1)(a+1) \equiv 0 \pmod p$ となるから．

それ以外の $p-3$ 個の数 $2, 3, \cdots, p-2$ はこの中に自分以外の mod$p$ での逆元 をもっているので，

$$(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdots (p-2)) \cdot (p-1) \equiv p-1 \equiv -1 \pmod p$$

である．

$\Longleftarrow$) 対偶を示す．p が素数でないとすると，$p = ab,\ 0 < a, b < p$ が存在するので，$(p-1)! \equiv 0 \pmod p$ である． □

§7.3 方程式 $x^2 + 1 \equiv 0 \pmod p$

定理 1.23 (オイラー). 奇素数 p について，$x^2 \equiv -1 \pmod p$ が解をもつこと[19]と，$p \equiv 1 \pmod 4$ であることは同値である

証明. $\Longrightarrow$) $x^2 \equiv -1 \pmod p \Longrightarrow x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}$ $\pmod p$ である．フェルマーの小定理により，$x^{p-1} \equiv 1 \pmod p$ だから，

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod p \text{ であり}, p | 1 - (-1)^{\frac{p-1}{2}}$$

[19]このことを「-1 は p を法として平方剰余である」と言う．

である．一方，$1-(-1)^{\frac{p-1}{2}}$ は 0 か 2 だが，p が奇素数なことから，0 しか取れない．つまり，

$$(-1)^{\frac{p-1}{2}} = 1 \Longleftrightarrow \frac{p-1}{2} \equiv 0 \pmod 2 \Longleftrightarrow p-1 \equiv 0 \pmod 4$$

とならねばならない．(注意：こちら側の証明にはウィルソンの定理はいらない．)

$\Longleftarrow$) $p \equiv 1 \pmod 4$ だから，$q = (p-1)/2$ は偶数である．P_p と $\{\pm 1, \pm 2, \cdots, \pm q\}$ は共に $\mathbb{Z}_p^\times$ の代表系だから，$x = q!$ とおけば，ウィルソンの定理により

$$-1 \equiv (p-1)! \equiv (-1)^q (q!)^2 = x^2 \pmod p$$

となる． □

§7.4 素数テストについて

与えられた数 n が素数であるかどうかを判定することは意外に難しい．ウィルソンの定理 1.22 を使えばよいようでも，n が素数かどうかを判定するために $(n-1)!$ の計算をしなければならない．$n!$ を計算してみればそれがいかに実際的でないかが分かるだろう．それよりは $\sqrt{n}$ までの素数で割ってみる方がずっと速い．

n 番目の素数 p_n の具体的な表示を求める試みは失敗の連続だが，少なくとも無限個の素数を 1 つの式で表わしたいという希望をもった人は多くいた．

フェルマーは $2^{2^n}+1$ はいつでも素数だと考えた．$n = 0, 1, 2, 3, 4$ は確かに素数になるが，$n = 5$ のときは 641 という素因数があることをオイラーが示した．じつは 2^n+1 の形の数が素数であるためには n が 2 のべきであることは必要条件であり，それを十分だ思ってしまったということらしい[20]．現在はこの形の素数をフェルマー (素) 数とよび，正多角形の作図問題と関

[20] 古今に名高い数学者といえども間違いをしてしまうこともある．大数学者とは間違いを恐れず未知の荒野を進んだ人たちであり，多くの間違いができたからこそ大数学者になり得たのだとも言える．フェルマーはその中にあって極端に間違いの少ない人なのだが，こうして間違いをする．高校生諸君も間違うことを恐れず，積極的に数学に取り組んでほしい．

係していることが知られている．

また，2^n-1 の形の数が素数であるためには n が素数であることが必要条件であり，この形の素数をメルセンヌ(素)数とよぶ．最大の素数(もちろん具体的な値として知られる)は，この形の数の中で探索されることが多い．また，偶数の完全数は，メルセンヌ数と同じだけしかないことも知られている．つまり，メルセンヌ数 2^n-1 に対する $2^{n-1}(2^n-1)$ は完全数で，偶数の完全数はこの形のものに限ることが，1849 年にオイラーによって示されている．

その他にも素数の候補は多く知られているし，興味あることも多いが，本書の内容とは違う流れなのでこの辺にしておく．詳しいことが知りたい読者には，リーベンボイム『素数の世界　その探索と発見』(1991) を薦めておく．

1 つだけ，多少実用的な素数テストを挙げておく．もちろん，奇素数を判定できればよい．2. は古典的な結果だが，1. はごく最近知られたものである．証明は初等的にできるが，さらに 10 ページほどの準備がいるので残念ながら省略する．

定理 1.24.

1. **(リフシッツ).** $p \equiv 1 \pmod 4$ **が素数のとき，** $q = 2p+1$ **が素数であることと，** q **が** 2^p+1 **を割り切ることとが同値である．**
2. **(オイラー，ラグランジュ).** $p \equiv 3 \pmod 4$ **が素数のとき，** $q = 2p+1$ **が素数であることと，** q **が** 2^p-1 **を割り切ることとが同値である．**

第 2 章

数列の密度

数列の密度の定義に実数の集合の「下限(かげん)」という概念が使われるので，定義を与えておく．

実数の集合 X のどの数より大きくない (小さいか等しい) 数 m があれば，m を X の**下界**(かかい)と言い，X は**下に有界**であるという．さらに最大の下界を**下限**といい，$\inf X$ と書くのであるが，実数論の基本的な事実として，下に有界な集合は下限をもつことがわかる[1]．X が下界をもたないときは $\inf X = -\infty$ とする．X が数列 $X = \{x_1, x_2, \cdots\}$ のときは下限 $\inf X$ を $\inf\limits_{n} x_n$ と書くことも多い．

つまり，x が集合 X の下限であるとは次の 2 つの条件を満たすときに言う，と言い更えることができる．

1)　すべての $a \in X$ に対して，$x \leqq a$ (x が X の下界であること)．

2)　$y > x$ であれば，$a < y$ となる $a \in X$ が存在する (x が下界として最大のものであること)．

以下に挙げられている命題を自分で証明しようとすれば，条件の 2) は，

2′)　任意の $\varepsilon > 0$ に対して，$a < x + \varepsilon$ となる $a \in X$ が存在する

という ε - δ 式の定義の方が便利なことがある．

[1] 少し厳密な微積分の本にはどれにも書いてあるが，[ハイラー，ワナー (1997)] を挙げておく．

§1　密度の性質

第 2 章では自然数の集合 $\mathbb{N}$ の無限部分集合 A を，その元の増大する順に並べて番号を付けることによって，単調増大な自然数列 $A = \{a_1, a_2, \cdots, a_n, \cdots\}$ と同一視している．

自然数の区間 $[a,\ b]$ を $\{n \in \mathbb{N} \mid a \leqq n \leqq b\}$ と定義する．

本文第 2 章 §1 で述べられた，単調増大な自然数列 $A = \{a_1, a_2, \cdots, a_n, \cdots\}$ の密度に関する 6 つの性質を証明する．その前に，言葉づかいを少し現代的なものに書き直すことにする．

自然数 $n \in \mathbb{N}^{\times}$ に対して，$A(n) = \#\{k \in A \mid 1 \leqq k \leqq n\} = \#(A \cap [1, n])$ とおく．区間 $[1,\ n]$ での A の密度 $A(n)/n$ の n に関する下限を A の**密度**と定義し，$d(A)$ と書いている．つまり，$d(A) = \inf\limits_{n} \dfrac{A(n)}{n}$ と定義されている．

一言で言えば，ある性質をもった自然数 (例えば，素数，偶数，3 の倍数，平方数，三角数など) が，自然数全体の中でどれくらい多いかという度合を表わすものである．

しかし，素朴な感覚とは馴染まない．例として，上に挙げたものはすべて密度が 0 である．奇数全体の密度は 1/2 だが，偶数全体の密度は 0 である．3 の倍数の密度は 0 だが，3 を法として 1 と合同な自然数全体の密度は 1/3 である．

また，$\mathbb{N}$ から 1 つの数 n を除いた集合 $\mathbb{N} \setminus \{n\}$ の密度が 1 であるというのが素直な感覚だと思うし，そう考える数学の理論もあるのだが，上の定義では $d(\mathbb{N} \setminus \{n\}) = \dfrac{n-1}{n} = 1 - \dfrac{1}{n}$ となって，除かれる数によってさえいる．

つまり，自然数の集合の密度の概念は (加法的) 整数論の議論にとって便利なように定義されているのである．むしろ，素直な感覚から離れて，このように密度を定義したことこそがこの分野におけるシュニレルマンの重要な貢献だというべきである．

本文第 2 章 §2 で証明が読者にゆだねられた命題は次のように書くことができる．

命題 2.1.

1. $a_1 > 1 \implies d(A) = 0$ **である．**

2. **自然数** $r \in \mathbb{N}$ **に対して** $a_n = 1 + r(n-1)\ (n = 1, 2, \cdots) \implies d(A) = \dfrac{1}{r}$ **である．**

3. **自然数** $r \in \mathbb{N}$ **に対して** $a_n = a_1 r^{n-1}\ (n = 1, 2, \cdots) \implies d(A) = 0$ **である．**

4. $a_n = n^2\ (n = 1, 2, \cdots) \implies d(A) = 0$ **である．**

5. $a_n = n\ (n = 1, 2, \cdots) \iff d(A) = 1$ **である．**

6. $d(A) = 0$ **かつ** $a_1 = 1$ **ならば，任意の** $\varepsilon > 0$ **と任意に大きな整数** $M > 0$ **に対して，整数** $N \geqq M$ **で，**

$$A(N) < \varepsilon N$$

を満たすものが存在する．

1. の証明

$a_1 > 1$ だから，$0 = A(1) = A(1)/1$ であり，$d(A) = \inf_n A(n)/n = 0$ である．

命題の直前のコメントの証明のためには，$A = \mathbb{N} \backslash \{n\}$ とおくとき，$A(k) = k\ (k < n),\ k - 1\ (k \geqq n)$ であることに注意すればよい．

2. の証明

$n \in \mathbb{N}$ に対して $a_k \leqq n \leqq a_{k+1} - 1$ となる k が存在し，そのとき $A(n) = k$ である．逆に，この範囲の n に対して

$$\frac{k}{a_{k+1} - 1} \leqq \frac{A(n)}{n} = \frac{k}{n} \leqq \frac{k}{a_k}$$

$$\frac{1}{r} = \frac{k}{kr} \leqq \frac{A(n)}{n} \leqq \frac{k}{1 + (k-1)r} = \frac{1}{r + (1-r)/k}$$

となる．$n = a_{k+1} - 1$ のとき左側の等号が成立する．したがって，$d(A) = \inf A(n)/n = 1/r$ である．

3. の証明

$a_1 > 1$ なら 1. により $d(A) = 0$ だから，$a_1 = 1$ と仮定してよい．すると $a_k = r^{k-1}$ である．2. の証明と同様に，$A(n) = k$ となるのは $a_k \leqq n \leqq a_{k+1} - 1$ のときだから，この範囲の n に対して

$$\frac{k}{r^k - 1} \leqq \frac{A(n)}{n} \leqq \frac{k}{r^{k-1}}$$

となる．両辺とも等号が成立する n はある．$k \to \infty$ とすると，単調に 0 に収束するので，$d(A) = \inf A(n)/n = 0$ である．

4. の証明

2. の証明と同様に，$A(n) = k$ となるのは $a_k \leqq n \leqq a_{k+1} - 1$ のときだから，この範囲の n に対して

$$\frac{1}{k} = \frac{k}{k^2} \geqq \frac{A(n)}{n} \geqq \frac{k}{(k+1)^2 - 1} = \frac{1}{k+2}$$

となる．両辺とも等号が成立する n はある．$k \to \infty$ とすると，単調に 0 に収束するので，$d(A) = \inf A(n)/n = 0$ である．

5. の証明

$a_n = n \ (n = 1, 2, \cdots) \iff A(n) = n \ (n = 1, 2, \cdots)$ である．一方，$0 \leqq A(n)/n \leqq 1$ に注意すれば，$d(A) = \inf A(n)/n = 1 \iff A(n)/n = 1 \ (n = 1, 2, \cdots)$ である．

6. の証明

$d(A) = \inf\limits_{n} A(n)/n = 0$ だから，どんなに小さな $\varepsilon > 0$ も $\{A(n)/n\}$ の下界にはなれず，$A(n)/n < \varepsilon$ となる n がある．この n が $n > M$ ととれればよいのだから，

$$\varepsilon' = \min\left\{\frac{A(1)}{1}, \frac{A(2)}{2}, \cdots, \frac{A(M)}{M}, \varepsilon\right\}$$

とおけば，$A(n) > 0$ であることから $\varepsilon' > 0$ になる．この ε' に対して上のような n をとって N とすればよい．

§2　素数の多さと少なさ

$x > 0$ に対して，$\pi(x) = \#\{p : 素数 \mid p \leqq x\}$ という値をもつ**素数関数**を定義する．また，素数を大きさの順に番号をつけて，$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11, \cdots$ などとする．$p_{1240} = 10099$ までの素数表を附録として与えておいた．n から何らかの方法で計算できる関数として p_n を与えるという問題は，不可能に近い．また明らかに，$\pi(p_n) = n$ である．

§2.1　素数は多い (ユークリッドとオイラー)

以下，記号で書くときの便利のために，素数全体の集合を $\mathbb{P}$ と書こう．集合 $\mathbb{P}$ の大きさや $\mathbb{N}$ の中での分布の仕方が問題になる．

定理 2.2 (ユークリッドの素数定理).　**素数は無限にある．つまり，$\lim_{n\to\infty} \pi(n) = \infty$.**

ユークリッドの証明.　素数が有限個しかない，例えば $r = \#\mathbb{P}$ であると仮定する．$N = p_1 p_2 \cdots p_r + 1$ を考えると，p_i は N を割らない (もし $p_i | N$ ならば $p_i | 1$ となるから)．N の素因数 (N が素数のときは N 自身) は $p_1, \cdots, p_r$ 以外の素数になり，矛盾する．□

ユークリッドの与えた証明は構成的ではあるが，知られている素数 $p_1, \cdots, p_r$ から得られる新しい素数はあまりに大きい．例えば，$q_1 = 2$, $q_2 = 3$ として，この手順で素数を作ってみよう．$2 \cdot 3 + 1 = 7$ は素数 ($q_3 = 7$)．$2 \cdot 3 \cdot 7 + 1 = 43$ も素数 ($q_4 = 43$)．$2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \times 139$ だから

$q_5 = 13$ とする．$2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 23479 = 53 \times 443$ だから $q_6 = 53$ とする．いくらでも続けられるが，コンピュータで計算してみても割と早くオーバーフローするだろう[2]．それはともかく，この方式で漏れ落ちる素数が非常に多いだろうということは分かる．

その話に移る前に，オイラーの証明を紹介しておく．微積分の初歩を知らないと難しく感じるかも知れないが，あまり気にしないで理解しようとして欲しい．整数の議論の中で，無限級数だけでなく無限積が有効であることをオイラーは示した[3]．

オイラーの証明． 素数が有限個，例えば r 個しかなかったと仮定する．等比級数の和の公式から

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \dfrac{1}{p_i}}$$

となるので，これをすべて掛けると (有限個としているので収束は問題はない)

$$\prod_{i=1}^{r} \sum_{k=0}^{\infty} \frac{1}{p_i^k} = \prod_{i=1}^{r} \frac{1}{1 - \dfrac{1}{p_i}}$$

となる．左辺は素因数分解の一意性定理 1.13 により，調和級数 $\displaystyle\sum_{n \geqq 1} \frac{1}{n}$ となり，無限大に発散することが分かっている[4]．ところが右辺は有限個の積

---

[2]コンピュータ自身の性能と，ソフトウェアの能力が上がればそれなりに長く続けられるが，多分読者が予期するよりもずっと早くオーバーフローするだろう．それでも，アルゴリズムや工夫によって少しでも多くの q_n を求めようとするのは，よい計算練習になる．

[3]これらが微積分の範囲だと感じるとすれば，それは単に学習の区分にすぎない．数学は 1 つである．

[4]積分を知っていれば，$\displaystyle\sum_{n=1}^{m} \frac{1}{n} \geqq \int_1^{m+1} \frac{1}{x}\,dx = [\log x]_1^{m+1} = \log(m+1) \to \infty$ $(m \to \infty)$ とするのが一番やさしい．

初等的にしたければ，$\mathbb{N}^{\times}$ を $\mathbb{N}^{\times} = \cup_{i=1}^{\infty} I_i$，$I_i = \{2^{i-1}+1, 2^{i-1}+2, \cdots, 2^i\}$ と分け

だから有限の値になることになり，矛盾する． □

§2.2 素数はもっと多い (ディリクレ)

第 1 章 §7 の定理 1.17 (オイラー) の系として，ディリクレの算術定理の特殊な場合が証明できる．

定理 2.3 (ディリクレの算術定理). $(a,b)=1$ **ならば，** a **を初項とし** b **を公差とする等差数列は無限個の素数を含む．**

これはまた,「$(a,b)=1$ ならば，$p \equiv a \pmod{b}$ の素数 p は無限に存在する」という言い方もできる．さすがにこの定理の証明は難しい．証明には，a を初項とする等差数列の中に素数を 1 つ見つければいいのだが，それが難しい．しかし，小さい b を特定すれば容易に証明できることもある．いくつか示してみよう．

定理 2.4.
1. $p \equiv 1 \pmod{4}$ **の素数** p **は無限に存在する．**
2. $p \equiv 3 \pmod{4}$ **の素数** p **は無限に存在する．**
3. $p \equiv 2 \pmod{3}$ **の素数** p **は無限に存在する．**

証明. 1. $1 \pmod{4}$ $(a=1,\ b=4)$ の場合．
素数の無限性のユークリッドの証明のまねをする．このような素数が有限個，例えば N 個だったとして，それをすべて，$p_1 < p_2 < \cdots < p_N$ と並べて，$M = (p_1p_2\cdots p_N)^2+1$ とおく．p を M の素因数とすると，$M = (p_1p_2\cdots p_N)^2+1 \equiv 0 \pmod{p}$ となるが，第 1 章 §7.3 のオイラーの定理 1.23 によって $p \equiv 1 \pmod{4}$ となる．しかし，どの p_i も M の約数ではないので，p は新しい素数である． □

2. $3 \equiv -1 \pmod{4}$ $(a=-1,\ b=4)$ の場合．

て，I_i の各元 x を一番大きな 2^i でおき換えて，$\displaystyle\sum_{x\in I_i}\frac{1}{x} \geqq \sum_{x\in I_i}\frac{1}{2^i} = \frac{1}{2^i}\times 2^{i-1} = \frac{1}{2}$ とすればよい．

そのような素数が有限個，例えば N 個だったとして，それをすべて，$p_1 < p_2 < \cdots < p_N$ と並べて，$M = 4(p_1 p_2 \cdots p_N) - 1$ とおく．奇数 M の素因数 q がもしもすべて $q \equiv 1 \pmod 4$ であれば，その積である M も $M \equiv 1 \pmod 4$ となるので，M の素因数のうち少なくとも 1 つは $\equiv -1 \pmod 4$ でないといけないが，それはまた，p_i のどれでもない． □

3.　$2 \pmod 3$ $(a = -1,\ b = 3)$ の場合．

どんな自然数 $n \equiv 2 \pmod 3$ の素因数の中にも，必ず $p \equiv 2 \pmod 3$ となるものがある (mod3 での掛算表を考えよ．n は 3 で割れず，$1 \cdot 1 \equiv 1 \pmod 3$ である) ことを注意しておく．

$q \geqq 3$ を $q \equiv 2 \pmod 3$ の形の最大の素数だったとする．2 から q までのすべての素数の積から 1 を引いた数を M とすると，$M \equiv -1 \equiv 2 \pmod 3$ であり，M の素因数はすべて q より大きい． □

§2.3　素数は少ない (オイラー)

素数の無限性のオイラーによる証明の中の式の右辺は，実際は有限個ではなく無限個の積であった．しかし，その値は定まるのだろうか．

補題 2.5.

$$\prod_{i=1}^{r} \frac{1}{1 - \dfrac{1}{p_i}} \to \infty \quad (r \to \infty)$$

証明.　無限級数や無限積の議論は慎重にする必要があるが，おおらかにするとすれば，

$$\begin{aligned}\prod_{p:\text{素数}} \frac{1}{1 - \dfrac{1}{p}} &= \prod_{p:\text{素数}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) \\ &= 1 + \prod_{p:\text{素数}} \frac{1}{p} + \prod_{p,q:\text{素数}} \frac{1}{pq} + + \prod_{p,q,r:\text{素数}} \frac{1}{pqr} + \cdots\end{aligned}$$

$$= \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

となる．

少し慎重にしたければ，

$$\begin{aligned}\prod_{i=1}^{r} \frac{1}{1-\frac{1}{p_i}} &= \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \frac{1}{{p_i}^3} + \cdots\right) \\ &= \sum_{e_1, e_2, \cdots, e_r \geqq 0} \frac{1}{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}} \\ &\geqq \sum_{n=1}^{p_r} \frac{1}{n} \to \infty \quad (r \to \infty)\end{aligned}$$

とすればよい． □

本文第 2 章 §2 で述べられている数列 $P = \{0, 1\} \cup \{p : \text{素数}\} = \{0, 1\} \cup \mathbb{P}$ の密度が 0 であることを示そう．$P(n)$ と素数関数 $\pi(n)$ は $P(n) = \pi(n) + 1$ という関係にあり，どんな $n \geqq 1$ に対しても $P(n) > 0$ なので，

$$d(P) = \inf_n \frac{P(n)}{n} = 0 \Leftarrow \lim_{n\to\infty} \frac{P(n)}{n} = 0 \Leftrightarrow \lim_{n\to\infty} \frac{\pi(n)}{n} = 0$$

である．したがって，次の定理 2.7 を示せばよい．

注意 2.6. 補題 2.5 で逆数を取れば，$\displaystyle\prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i}\right) = 0$ となるが，無限積 $\displaystyle\prod_{i=1}^{\infty}(1 - a_i)$ の収束と無限和 $\displaystyle\sum_{i=1}^{\infty} a_i$ の収束が同値だというよく知られた事実により[5]，$\displaystyle\sum_{p:\text{素数}} \frac{1}{p} = \infty$ であることが分かる．これは例えば，オイラーの示した $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ という式[6]と比べれば，素数が平方数よりもはるか

[5] 大抵の微積分の教科書に載っている．

に多いことを意味していることになる．また，附録の数表を見て実感して欲しい．

定理 2.7 (オイラーの素数定理). $\displaystyle\lim_{n\to\infty}\frac{\pi(n)}{n}=0.$

証明. 単に極限をとるという議論だけでこれを証明するのは難しい．任意に (小さい) $\varepsilon>0$ を与えたとき，十分大きな n に対して[7]，$\dfrac{\pi(n)}{n}<\varepsilon$ が成り立つを示すことにする[8]．

さて，上の注意により，任意に与えた小さい $\varepsilon>0$ に対して，十分大きな r に対しては $\displaystyle\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)<\varepsilon$ となっている．この r を止めておいて，n を大きくすることを考える．

$q=\displaystyle\prod_{i=1}^{r}p_i$ とおくと，定理 1.19 により，$\varphi(q)=q\displaystyle\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$ だから，$\varphi(q)/q<\varepsilon$ となっている．

n を q で割って，

$$n=sq+t\ \ (0\leqq t<q)$$

とする．整数の区間 $[1,n]$ を

$$[1,n]=\bigcup_{i=1}^{s}I_i\ \cup\ [sq+1,n],\qquad I_i=[(i-1)q+1,\ iq]$$

と分割する．$I_1=[1,q]$ の中の素数 p は $\{p_1,\cdots,p_r\}$ のどれかであるか，または $(p,q)=1$ を満たす．$\varphi(q)=\#\{m\in[1,q]\mid(m,q)=1\}$ であったことを思い起こすと，$\pi(q)\leqq r+\varphi(q)$ である．$i>1$ のときの I_i の中の素数

---

[6]証明は，たとえば，ハイラー，ワナー『解析教程　上』第 I 章 §5 の (5.31) 式やアイグナー，ツィーグラー『天書の証明』第 6 章定理 3 にある．

[7]五月蝿くいえば,「ある N があって，すべての $n>N$ に対して」ということになる．大学の微積分の講義でも一番理解されにくい箇所の 1 つである．

[8]$a\geqq 0$ がどんな正の ε よりも小さければ，$a=0$ とならざるをえない．もし $a>0$ ならば，$\varepsilon=a/2$ とおくと $a<\varepsilon$ を満たさない．

p も $(p,q)=(p-(i-1)q,q)=1$ を満たしており，その個数は $\varphi(q)$ 以下である．したがって，

$$\pi(n) \leqq r + s\varphi(q) + q$$

である．$n = sq + t$ で割ると

$$\frac{\pi(n)}{n} \leqq \frac{r+s\varphi(q)+q}{n} \leqq \frac{r+q}{n} + \frac{s\varphi(q)}{sq} < \frac{r+q}{n} + \varepsilon$$

となる．$\dfrac{r+q}{n}$ も，r を止めて n を大きくするのだから 0 に近付いていき，十分大きな n に対しては $<\varepsilon$ となっている．こうして，任意に与えた $\varepsilon>0$ に対して，十分 n が大きければ $0 \leqq \dfrac{\pi(n)}{n} < 2\varepsilon$ となっているのだから，$\displaystyle\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$ となる． □

§2.4　素数は多いか少ないか

$\pi(x)$ が $x\to\infty$ のときにどう振る舞うかについて，さらに詳しいことがガウスによって予想され (1792)，多くの数学者が攻略に参加し，1896 年に J. アダマールとドゥ・ラ・ヴァレ・プーサンが独立に証明した．今日，**素数定理**といえば，この

$$\pi(x) \sim \frac{x}{\log x} \quad (x\to\infty)$$

という事実を指すことが多い．関心の高いこの定理には多くの証明が知られている．長い間解析的な証明しか知られていなかったが，1949 年にこれもまた独立にエルデシュとセルバーグにより，整数論的関数の初等的評価のみを使った証明が与えられた[9].

さらに詳しい結果もある．例えば，$\pi(x)-\dfrac{x}{\log x}$ の漸近挙動とか，リーマンのゼータ関数などに発展していく．ここでは，少ない予備知識で述べら

---

[9] 初等的とはいっても，ここに挙げることができるほど簡明ではない．証明を知りたければ，訳者まえがきで挙げた本のどれかもしくは原論文を見られたい．

れる周辺のことがらを述べておくことにする．

第1章のファン・デル・ヴェルデンの定理を，素数 $\mathbb{P}$ と合成数 $\mathbb{N}\setminus\mathbb{P}$ のクラスに分けたとして使えば，どんな長さの等差数列もどちらかにはあることになる．確かに公差を $k \geqq 2$ とすると，k が素数であれ合成数であれ，$\{nk \mid n \geqq 2\}$ は公差 k の無限等差数列で，すべて合成数である．さらに，**どんな $N \geqq 1$ に対しても，公差 1 で長さ N の合成数だけからなる等差数列** (この場合は区間) **がある**ことも分かる．実際，N 個の数 $(N+1)!+2,\ (N+1)!+3,\ \cdots,(N+1)!+N+1$ はすべて合成数である． □

素数の側では，例えば「**各自然数 M に対し，ある自然数 k が存在し，差が $2k$ である連続する素数の組が M 個以上存在する**」ことが言える．証明は素数定理を使って，十分大きな n に対しては，差の集合 $\{p_{i+1}-p_i \mid 2 \leqq i \leqq n\}$ の元の個数が $(n-2)/M$ より小さいことを示せばよい． □

また，P の中にも任意の長さの等差数列がとれることや

$$\lim_{n\to\infty}(\sqrt{p_{n+1}}-\sqrt{p_n})=0$$

も成り立つことが期待されている予想である．これが成り立てば「**k が十分大きければ，k^2 と $(k+1)^2$ の間に必ず素数が存在する**」という予想を示すことができる．実際，k_i^2 と $(k_i+1)^2$ の間に素数が存在しないような無限列 $k_1<k_2<\cdots$ が存在したとする．k_i^2 を越えない最大の素数を p_{h_i} とすると，$p_{h_i+1}>(k_i+1)^2$ となる．したがって，

$$\sqrt{p_{h_i}}<k_i<k_i+1<\sqrt{p_{h_i+1}}$$

を満たす $h_1<h_2<\cdots$ があることになるが，これは上の極限式に矛盾する．

□

§2.5 ベルトランの仮説

前の小節の最後の予想に似たものにベルトランの仮説 (1845) があり，これは 1852 年に初めてチェビシェフによって証明された．

定理 2.8 (ベルトランの仮説，チェビシェフの定理)． 任意の自然数 $n \geqq 2$ と $2n$ の間に必ず素数がある (これは $p_{m+1} < 2p_m \ (m \geqq 1)$ とも同値である)．

附録の素数表を見ながら，$q_1 = 2$ から初めて，帰納的に $2q_{k-1}$ を越えない最大の素数 q_k が q_{k-1} より大きいことが分かればよい．実際にそういう列 $q_1, q_2, \cdots$ が得られれば，証明は済む．任意の自然数 n を越えない最大の q_k を取ると，$2q_k \leqq 2n$ であることと q_k の取り方から $n < q_{k+1} < 2n$ であることが分かる．

実際に q_k を求めてみよう．

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, \cdots$$

である．上の議論を使えば，$n < 9972$ に対してはベルトランの仮説が成り立つことになる．これが無限に続けられれば証明は終るのだが，それは無理なことである．それにしても思ったよりもずっと少ない計算で，多くのことが証明できたような感じがするが，これを**ランダウのトリック**という．

エルデシュ(1930) による初等的な証明を紹介しよう．ただし，2 項係数に関する評価を使うので，まずそれをまとめておく．$n \geqq 3$ に対して

$$\binom{2n}{n} > \frac{4^n}{2n} \tag{B1}$$

$$\binom{2n}{n} \leqq \prod_{p \leqq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leqq \frac{2}{3}n} p \cdot \prod_{n < p \leqq 2n} p \tag{B2}$$

が成り立つことが分かり (上式のように書いた積は条件を満たすすべての素数 p にわたってとるものとする)，この 2 式から

$$4^n \leqq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leqq \frac{2}{3}n} p \cdot \prod_{n < p \leqq 2n} p \tag{B3}$$

が得られる．(B1,2) 式と後で述べる (B4) 式の証明は後回しにして，まず，

ベルトランの仮説を証明しよう．

仮定法で示そう．ある $n \geqq 3$ に対して $n < p \leqq 2n$ となる素数が存在しなかったとしよう．すると，(B3) 式から

$$4^n \leqq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leqq \frac{2}{3}n} p$$

が得られる．さらに，不等式

$$\prod_{p \leqq x} p \leqq 4^{x-1} \qquad (x \geqq 2 \text{ は実数}) \tag{B4}$$

を使えば，

$$4^n \leqq (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n}$$

つまり

$$4^{\frac{n}{3}} \leqq (2n)^{1+\sqrt{2n}} \tag{B5}$$

が得られるが，この式は n が十分大きいと成り立たない．実際，$a+1 < 2^a (a \geqq 2)$ という不等式[10]を使えば，

$$2n = (\sqrt[6]{2n})^6 < \left(\left[\sqrt[6]{2n}\right] + 1\right)^6 < 2^{6\left[\sqrt[6]{2n}\right]} \leqq 2^{6\sqrt[6]{2n}} \tag{B6}$$

が得られ，だから，$n \geqq 50$(このとき $18 < 2\sqrt{2n}$ である) に対して，(B5) と (B6) とから，

$$2^{2n} \leqq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}$$

が得られる．指数を比較して，$(2n)^{1/3} < 20$ が得られ，$n < 4000$ となる．その場合の n に対してはすでにベルトランの仮説が成り立っていた． □

残った (B1,2,4) 式の証明をしていこう．

[10] この不等式がすべての $a \geqq 2$ に対して成り立つことは，帰納法によって容易に示すことができる．

(B4) の証明.　まず，q が $q \leqq x$ を満たす最大の素数なら，

$$\prod_{p \leqq x} p = \prod_{p \leqq q} p \quad \text{かつ} \quad 4^{q-1} \leqq 4^{x-1}$$

となるので，$x = q$ が素数の場合にだけ (B4) を証明すればよい．$q = 2$ のときは明らかだから，以下奇素数 $q = 2m + 1$ として考えると，

$$\prod_{p \leqq 2m+1} p = \prod_{p \leqq m+1} p \cdot \prod_{m+1 < p \leqq 2m+1} p \leqq 4^m \cdot \binom{2m+1}{m} \leqq 4^m 2^{2m} = 4^{2m}$$

となる．実際，不等式の最初の部分は帰納法の仮定であり，

$$\prod_{m+1 < p \leqq 2m+1} p \leqq \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m}$$

という不等式は，$\dfrac{(2m+1)!}{m!(m+1)!}$ が整数であり，積に現れる素数 p は分子 $(2m+1)!$ の素因数であって，分母 $m!(m+1)!$ には含まれないことから，また最後の不等式は，

$$\binom{2m+1}{m} = \binom{2m+1}{m+1} \leqq \sum_{k=0}^{2m+1} \binom{2m+1}{k} = (1+1)^{2m+1} = 2^{2m+1}$$

であることから分かる．□

(B1) の証明.　パスカルの三角形を考えて，第 $2n$ 段目だけ見れば

$$1 = \binom{2n}{0} < \binom{2n}{1} < \cdots < \binom{2n}{n} > \cdots > \binom{2n}{2n-1} > \binom{2n}{2n} = 1$$

となっている．両端の 1 を合わせて 1 項と考えるとき，真中にある一番大きな項 $\binom{2n}{n}$ は総和の $(1+1)^{2n} = 2^{2n} = 4^n$ を項数 $2n$ で割った平均値以上の値になる．□

(B2) の証明.　$n!$ の素因数分解に現れる素因数の個数に関するルジャン

ドルの定理 1.15 (第 1 章 §4.1) を使うと，$\begin{pmatrix} 2n \\ n \end{pmatrix}$ の素因数分解に現れる素因数 p の個数 e_p は

$$e_p = \sum_{k \geqq 1} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right)$$

となる．しかもその各項は整数であり，

$$\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) < 2$$

から，高々1 になる．

したがって，$e_p \leqq \displaystyle\sum_{k \geqq 1, p^k \leqq 2n} 1 = \max \{ k \geqq 1 \ : \ p^k \leqq 2n \}$ に注意すれば，

$$p^{e_p} \leqq \max \{ p^k \ : \ k \geqq 1, p^k \leqq 2n \} \leqq 2n$$

であること，さらに $p > \sqrt{2n}$ のときは $e_p \leqq 1$ であることが分かる．最後に (ここがポイント)，$\dfrac{2}{3} n < p \leqq n$ のときは $e_p = 0$ となる．実際，$3p > 2n$ だから $\begin{pmatrix} 2n \\ n \end{pmatrix} = \dfrac{(2n)!}{n!n!}$ の分子の p の倍数は p と $2p$ しかないが，分母にも p が 2 度現れる． □

注意.　p が素数のとき，具体的な値は分からないが $2p$ までに素数があるというのが定理の内容だが， ではその次の候補である $2p+1$ はどうなるのだろうか？　その解答が定理 1.24 であった．

§2.6　双子素数

p と $p+2$ が共に素数であるとき，これを**双子素数**という．古代からよく知られており，附録の素数表を見て調べてみると，予期したよりも多くの双子素数がある．たとえば，最初の方は

$$3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61;$$

$$71, 73; 101, 103; 107, 109; 137, 139$$

とほとんど軒並みであり，1000を越えても

$$1019, 1021; 1031, 1033; 1049, 1051; 1061, 1063;$$
$$1091, 1093; 1151, 1153; 1229, 1231$$

とあり，5000を越えたあたりで

$$5009, 5011; 5021, 5023; 5099, 5101; 5231, 5233;$$
$$5417, 5419; 5441, 5443; 5477, 5479$$

と少し減ってくるが，10000 近くでも

$$9719, 9721; 9767, 9769; 9929, 9931; 10007, 10009;$$
$$10037, 10039; 10067, 10069$$

などとあり，素数表に印をつけていけば真っ赤になった印象がするほどである．

素数関数と同様，$\pi_2(x)$ を x 以下の差が 2 の素数対の個数とすると，

$$\pi_2(10) = 2, \pi_2(10^2) = 8,\ \pi_2(10^3) = 35, \pi_2(10^4) = 205,$$
$$\pi_2(10^5) = 1224, \pi_2(10^6) = 8169, \pi_2(10^7) = 58980, \pi_2(10^8) = 440312,$$
$$\pi_2(10^9) = 3424506,\ \pi_2(10^{10}) = 27412679,\ \pi_2(10^{11}) = 224376048$$

であることが知られており，素数全体と同じように無限個あると予想されている．

この**双子素数予想**はまだ証明されていない．この方向での現在の最良の結果は，チェン (陳景瀾，1973/78) によるもので,「p が素数で $p+2$ が高々2つの素数の積であるような p は無限個ある」というものである．

逆にそれほどは多くないという結果もある．V. ブルン (1919a) はエラトステネスのふるいを改良して，

$$\sum_{p, p+2 \in \mathbb{P}} \left(\frac{1}{p} + \frac{1}{p+2} \right)$$

が収束することを示した．この値 B は**ブルン定数**とよばれており，1976 年の時点では $B = 1.90216054\cdots$ という計算がある．また V. ブルン (1919) は上からだけではあるが，

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

という素数定理と類似の評価を得ている．

またコンピュータと素数判定法の進歩によって，大きな双子素数を見つける競争も行われている．主な参加者は，Dubner, Atkin, Rickert, Keller, B.Parady, J.Smith, S.Zarantonello であり，1983 年までで最大桁数だったのは 1358 桁の $219649815 \times 2^{4481} \pm 1$ であり，1985 年には 2259 桁の $107570463 \times 10^{2250} \pm 1$ が，1990 年には 2389 桁の $1706095 \times 2^{11235} \pm 1$ が求まっている．また，1993 年には 4030 桁の $1691232 \times 1001 \times 10^{4020} \pm 1$ が求まっており，記録は次々と塗り替えられている．

最近はインターネットで刻々と記録が報告されていて，アメリカ，テネシー大学マルチン分校のホームページ (http://www.utm.edu/research/primes/largest.html) には，いろいろな素数の記録が掲載されている．それによれば，1999 年末での最大の双子素数は，11755 桁の $361700055 \times 2^{39020} \pm 1$ である (アンリ・リフシッツ，1999)．原稿の整理をしているうちに進展があり，2000 年 3 月末の段階では，18075 桁の $2409110779845 \times 2^{60000} \pm 1$ が世界記録である (Wassing, Járai, Indlekofer, 2000)．これも計算機の進展とともに一過性の記録になるということかも知れない[11]．

[11] 双子素数でなく 1 つの素数だということなら探索もさらに進み，2000 年 3 月末の時点で知られている最大の素数は $2^{6972593} - 1$ というメルセンヌ素数で，2098960 桁という膨大なものである (Hajratwala, Woltman, Kurowski, GIMPS, 1999)．

第 3 章

整数の和表示

§1 から §6 までは，整数をいくつかの平方数の和に書くことに関するものである．$g(k)$ や $G(k)$ の意味については，本文第 2 章の初めの脚注を参照すること．

§1 平方数の和の積を平方数の和に書く公式

以下で，平方数の和に関する定理を証明するときのキーになる公式を 2 つ挙げておく．

命題 3.1.

1. 任意の実数 x_1, x_2, y_1, y_2 **に対して**

(Q2) $$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$$

と

(Q2′) $$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$$

が成り立つ．

2. 任意の実数 $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ **に対して**

(Q4)

$$\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\
&= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
&\qquad + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2
\end{aligned}$$

が成り立つ.

証明. 直接展開しても示せるが[1]，次のように考えると分かりやすい.

1. 複素数 $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$ とおけば，(Q2) の左辺は $|z_1|^2|z_2|^2$ であり，右辺は $|z_1\bar{z}_2|^2$ である．また z_2 と掛けて，$|z_1|^2|z_2|^2 = |z_1z_2|^2$ を計算すれば (Q2′) が得られる.

2. また，四元数 $x = x_1 + ix_2 + jx_3 + kx_4$ $(x_i \in \mathbb{R})$ を考えると，同様にして等式 (Q4) が得られる.

複素数の集合 $\mathbb{C}$ が $i^2 = -1$ を満たす i を実数 $\mathbb{R}$ に付け加えたものだったように，四元数の集合は

$$i^2 = j^2 = k^2 = -1,\ ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik$$

を満たす i, j, k を実数 $\mathbb{R}$ に付け加えたものである[2].

複素数が (x_1, x_2) と $x = x_1 + ix_2$ を対応させて平面の点として表わすことができたように，四元数は (x_1, x_2, x_3, x_4) と $x = x_1 + ix_2 + jx_3 + kx_4$ を対応させて 4 次元空間の点として表わすことができる.

複素数 x の絶対値 $|x| = \sqrt{x_1^2 + x_2^2}$ が，x に対応する平面の点の原点との距離だったように，四元数 x の絶対値 $|x| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$ は，x に対応する 4 次元空間の点の原点との距離である．また，共役四元数を $\bar{x} = x_1 - ix_2 - jx_3 - kx_4$ とおけば，$|x|^2 = x\bar{x} = |\bar{x}|^2$ となる.

このとき，$y = y_1 + iy_2 + jy_3 + ky_4$ を考え，$z = x\bar{y}$ を計算すれば，

(Q4z)

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \qquad z_2 = -(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3),$$

$$z_3 = -(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4),\ z_4 = -(x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)$$

となり，等式 (Q4) は $|x|^2|y|^2 = |x\bar{y}|^2$ に他ならない. □

---

[1]高校生である読者なら，一度くらいは実際に展開計算をするとよい．計算して初めて，計算だけしていてはいけないことが分かることもある.

[2]四元数についてより詳しいことが知りたければ，たとえば G. トス『数学名所案内 下』(1998) の第 21 節を見るとよい.

§2　2つの平方数の和 (フェルマーの定理)

定理 3.2 (フェルマー).　あらゆる素数 $p \equiv 1 \pmod 4$ は 2 つの平方数の和に書ける.

この定理は，有名なフェルマーの無限降下法の実例としても興味深い．有名なこの証明法は，例えば，次のように使われる．

f を 2 次形式とし，方程式 $f(x_1, \cdots, x_n) = m$ の整数解を求めたいとする．帰納法の第 1 段階として，ある $k > 0$ に対して，方程式 $f(x_1, \cdots, x_n) = km$ の整数解が存在することを示す．第 2 段階として，$k > 1$ であれば，ある $0 < k' < k$ を探して，方程式 $f(x_1, \cdots, x_n) = k'm$ の整数解が存在することを示す．

命題 $P(k)$ を「方程式 $f(x_1, \cdots, x_n) = km$ は整数解をもつ」として，定理 1.6 (MI3) を使うのである．

§2.1　無限降下法による証明

素数 p が $p \equiv 1 \pmod 4$ を満たせば，$\dfrac{p-1}{2}$ は偶数であり，オイラーの定理 1.23 によって，$x^2 \equiv -1 \pmod p$ は解をもつ．

このとき，x として $0 < x < p$ のものがとれるのは明らかだが，さらに $0 < x < p/2$ ととれる．というのも，もし，$p/2 < x < p$ ならば，$x' = p - x$ とおけば，$0 < x' < p/2$ かつ $x'^2 = p^2 - 2px + x^2 \equiv x^2 \equiv -1 \pmod p$ となるから．

すると，$k > 0$ があって，$x^2 + 1 = kp$ となるのだが，$0 < x < p/2$ と取ってあるので，$k < p$ となっている (ここで，$p \geqq 5$ に注意する)．

つまり，

$$(*) \qquad x^2 + y^2 = kp$$

には整数解があることになり，これが無限降下法の第 1 段階になる．$k = 1$

なら証明は終る．$k>1$ として議論を進める．

$(*)$ の解 x_0, y_0 を取り，$\mathrm{mod} k$ で合同な数のうち絶対値が最小のものを，それぞれ x_1，y_1 とすると，当然 $|x_1|$，$|y_1| \leqq k/2$ であり，$x_1^2+y_1^2 \equiv 0 \pmod k$ である．したがって，上の議論と同様にして，k' $(0<k'<k)$ があって，

$$(*1) \qquad x_1^2+y_1^2=k'k$$

を満たしている．$(*)$ と $(*1)$ を掛けると，(Q2) により，

$$(*2) \qquad k'k^2p=(x_0^2+y_0^2)(x_1^2+y_1^2)=(x_0x_1+y_0y_1)^2+(x_0y_1-x_1y_0)^2$$

となるが，この右辺の和の各項は

$$x_0x_1+y_0y_1 \equiv x_0^2+y_0^2 \equiv 0, \quad x_0y_1-x_1y_0 \equiv x_0y_0-x_0y_0=0 \pmod k$$

となる．そこで，

$$x_2=\frac{x_0x_1+y_0y_1}{k}, \qquad y_2=\frac{x_0y_1-x_1y_0}{k}$$

とおけば，$(*2)$ 式を k で割って，$x_2^2+y_2^2=k'p$ が得られる．無限降下法の第 2 段階が完成したことになり，いつか $x^2+y^2=p$ の解が得られることになる． □

§2.2 無限降下法によらない証明

このように多くの人の関心を集めた定理にはいろいろな証明法が知られていることがある．帰納法を使わない直接的な証明を紹介しよう．しかし，そのために 1 つの補題を準備しなければならない．

補題 3.3. **任意の実数** $\xi \in \mathbb{R}$ **と任意の自然数** $n \in \mathbb{N}$ **に対して，整数** $k(\leqq n), h \in \mathbb{Z}$ **が存在して，**

$$\left|\xi-\frac{h}{k}\right| \leqq \frac{1}{k(n+1)}$$

を満たす．

証明． 普通は連分数論を使って証明されるが，ディリクレの引き出し論法を使う証明を紹介する．

区間 $I=[0,1]$ を $n+1$ 等分して，$I_i=[i/(n+1),(i+1)/(n+1)]$, $(0 \leqq i \leqq n)$ とおく．

n 個の点 $x_i=\xi i-[\xi i]$ $(1 \leqq i \leqq n)$ は，区間 $I=[0,1]$ の点である．

ある i があって，$x_i \in I_0$ なら，$|x_i| \leqq 1/(n+1)$ であり，$k=i$, $h=[\xi i]$ とおけば，$|\xi k-h| \leqq 1/(n+1)$ であり，$|\xi-h/k| \leqq 1/k(n+1)$ となる．

ある j があって，$x_j \in I_n$ なら，$|x_j-1| \leqq 1/(n+1)$ であり，$k=j$, $h=[\xi j]+1$ とおけばよい．

したがって，n 個の点 x_i, $(1 \leqq k \leqq n)$ は，I_0 と I_n には入っていないとしてよい．すると，(引き出し論法により) $n-1$ 個の小区間 I_j $(1 \leqq j \leqq n-1)$ のどれかには少なくとも 2 点が入っていなければならないことになる．つまり，$1 \leqq k_1 < k_2 \leqq n$ が存在して，

$$|(\xi k_2-[\xi k_2])-(\xi k_1-[\xi k_1])| < \frac{1}{n+1}$$

となる．このとき，$k=k_2-k_1>0$, $h=[\xi k_2]-[\xi k_1]$ とおけば，

$$|\xi k-h| < \frac{1}{n+1}$$

となる．$k>0$ だから，k で割ればよい． □

定理 3.2 (フェルマー) の別証． $p \equiv 1 \pmod 4$ だから，$x^2 \equiv -1 \pmod p$ は整数解をもつので，そのうち絶対値が最小のものを x とする．

実数 $\xi=-x/p$ と整数 $n=[\sqrt{p}]$ に対して，上の補題を適用すれば，整数 $0<b \leqq n < \sqrt{p}$ (p が素数だから) と a が存在して

$$\left|-\frac{x}{p}-\frac{a}{b}\right| \leqq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}$$

となる．$c=bx+ap$ とおき，上の不等式の両辺を bp 倍すると，$|c|<\sqrt{p}$

が得られる．$c \equiv bx \pmod p$ だから

$$b^2 + c^2 \equiv b^2 + (bx)^2 = b^2(1+x^2) \equiv 0 \pmod p$$

であるが，一方 $b^2 + c^2 < p + p = 2p$ だから，$b^2 + c^2 = p$ でなければならない． □

§2.3 1 文による証明

定理 3.2 のザギエ (1990) による証明は，次のたったの 1 つの文章からなるものである．

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & x < y-z \text{ のとき} \\ (2y-x, y, x-y+z) & y-z < x < 2y \text{ のとき} \\ (x-2y, x-y+z, y) & 2y < x \text{ のとき} \end{cases}$$

で定義される，有限集合 $S = \{(x,y,z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ の対合はただ 1 つの固定点をもち，それゆえ $|S|$ は奇数であり，$(x,y,z) \mapsto (x,z,y)$ で定義される対合もまた固定点をもつ．

確かに 1 つの文であり，名人芸である．しかし，鑑賞するには若干の予備知識が必要だ．簡単に説明しておこう[3]．

集合 S は有限集合になり，それが $S_1 = \{x < y - z\}$，$S_2 = \{y - z < x < 2y\}$，$S_3 = \{2y < x\}$ という 3 つの部分集合に分かれている．この 3 つの部分集合は互いに共通点をもたないが，それは p が素数であることから分かる．

第 1 の写像を f と書くとき，$f(S) \subset S$ であること，$f(S_1) \subset S_3$，$f(S_2) \subset S_2$，$f(S_3) \subset S_1$ であること，さらに**対合** ($f^2 = id_S$ を満たす写像のこと) であることは簡単な計算で分かる．f の固定点[4]は S_2 の点で，$p = 4n + 1$

---

[3] ［訳註］アイグナー，ツィーグラー『天書の証明』の「数論」の第 5 節にカラー図版のある説明があるので，詳しくはそちらを見られたい．

[4] f の固定点とは f によって固定される点，つまり $f(x) = x$ を満たす点 x のこと．

と書くとき $(1,1,n)$ しかないこともすぐに分かる．

また，2 つ目の写像の固定点 (x,y,z) は $y=z$ となっているので，$x^2+4y^2=p$ を満たしている．

後は，対合に関する一般的な命題

$f:S\to S$ を有限集合の対合とするとき，S と固定点の集合 $S^f=\{s\in S\mid f(s)=s\}$ の元の個数のパリティは等しい．

を使えばよい．このことは，f の固定点でない点 $s\in S\setminus S^f$ は，必ず $f(s)\neq s(=f^2(s))$ と対になっているので，$|S\setminus S^f|$ が偶数になることから分かる．

□

この証明は見事ではあるが，与えられた素数に対してどのような分解があるのかは一切教えてくれない．それには，アメリカ数学月報の同じ号に載っているワーゴン (1990) の解説が応えてくれる．

§2.4　2 つの平方数の和で書ける素数

まず，フェルマーの定理 3.2 からすぐに分かることとして，

定理 3.4.　**p を素数とする．p が 2 つの平方数の和で書ける $\iff$ $p=2$ または $p\equiv 1 \pmod 4$．**

証明.　$\Longleftarrow$ は，$2=1^2+1^2$ と定理 3.2 から．

$\Longrightarrow$ は，任意の自然数 n に対して $n^2\equiv 0,\ 1 \pmod 4$ であることから．

□

定理 3.5.　**p が 2 つの平方数の和で書ける素数とするとき，その書き方は本質的に 1 通りである．つまり，$p=x^2+y^2$，$x,y\in\mathbb{N}$，$2\nmid y$ を満たす x,y は一意的に定まる[5]．**

---

[5] じつはこの 2 つの定理に平行して，「p を素数とする．p が 2 つの平方数の差で書ける $\iff$ $p\neq 2$」という事実がなりたち，さらにその表示が一意的であることもわかる．

この証明はやさしい．答だけ書いておくと，$p=a^2-b^2$ と書けたとすれば，$a=(p+1)/2$，$b=(p-1)/2$ となる．

証明. $p=2=1+1$ のときは明らかだから，$p \equiv 1 \pmod 4$ とする．定理 3.4 により，$p=x^2+y^2$ を満たす偶数 x と奇数 y が存在する．p が素数だから，$(x,y)=1$ となる．ここで，$p=a^2+b^2$ を満たす偶数 a と奇数 b が存在したとして，$x=a, y=b$ を示そう．

$$(bx+ay)(bx-ay)=b^2x^2-a^2y^2=b^2(x^2+y^2)-(a^2+b^2)y^2=p(b^2-y^2)$$

であり，p は素数だから，$p|(bx+ay)$ または $p|(bx-ay)$ である．

$p|(bx+ay)$ ならば，ある $k \geqq 1$ があって，$bx+ay=kp$ であるが，$p^2=(a^2+b^2)(x^2+y^2)$ に (Q2′) 式を適用すると，

$$p^2=(ax-by)^2+(bx+ay)^2 \geqq k^2p^2$$

が得られ，$k=1$ かつ $ax-by=0$ となる．これから $ax=by$ が得られるが，仮定より偶数と奇数が等しいことになって矛盾．この場合は起こらない．

$p|(bx-ay)$ ならば，ある $k \in \mathbb{Z}$ があって，$bx-ay=kp$ であるが，$p^2=(a^2+b^2)(x^2+y^2)$ に (Q2) 式を適用すると，

$$p^2=(ax+by)^2+(bx-ay)^2 > k^2p^2$$

が得られ，$k=0$，ゆえに $bx=ay$ が得られる．$(a,b)=1$ であるから，$a|x$, $b|y$ となる．条件式から $x=ah$, $y=bh$ となり，これを p の表示式に代入すれば，$h=1$ となる． □

§2.5 2 つの平方数の和で書ける数

フェルマーの定理 3.2 の系として，2 つの平方数の和で書ける数の特徴づけが次のように得られる．

定理 3.6. **自然数 n が 2 つの平方数の和で書ける $\Longleftrightarrow$ n の素因数分解に現れる mod4 で 3 であるような素因数は偶数ベキである．**

証明. $\Longleftarrow$: n の素因数分解が

$$n=2^{e_2}p_1p_2\cdots p_sq_1^2\cdots q_t^2, \quad p_i \equiv 1,\ q_j \equiv 3 \pmod 4$$

であるとする．定理 3.4 と積公式 (Q2) から $2^{e_2}p_1p_2\cdots p_s = a^2+b^2$ と書けることがわかるので，

$$n = (aq_1\cdots q_t)^2 + (bq_1\cdots q_t)^2$$

と書ける．

$\Longrightarrow$：対偶を示す．$n = mq^{2k+1}$, $k \geqq 0$, $(q,m)=1$, $q \equiv 3 \pmod 4$ で，q は奇素数とする．n が $n = a^2+b^2$ と書けたと仮定して矛盾を導こう．$q \nmid a$ かつ $q \nmid b$ としてよい．なぜなら，$q|a$ ならば，$q|b$ となり，$k>0$ であることがわかり，$(a/q)^2+(b/q)^2 = mq^{2k-1}$ とおく．まだ駄目なら，これを繰り返す．

さてそうすると，$a^2 \equiv -b^2 \pmod q$ となるが，$q \nmid b$ だから，$bc \equiv 1 \pmod q$ となる自然数 c があるので，

$$(ac)^2 \equiv a^2c^2 \equiv -b^2c^2 \equiv -(bc)^2 \equiv -1 \qquad \pmod q$$

となり，オイラーの定理 1.23 に矛盾する． □

§3　$G(2) \geqq 4$ の証明

$G(2) \geqq 4$ であることは次の命題の系としてただちに得られる．

命題 3.7.　$n = 8k+7$, $k \in \mathbb{Z}_{\geqq 0}$ **は 3 つ以下の平方数の和に書けない．**

証明.　$(2i+1)^2 = 4i^2+4i+1 = 4i(i+1)+1 \equiv 1 \pmod 8$ であり，$(2i)^2 = 4i^2 \equiv 0$ または $4 \pmod 8$ となるので，平方数の和で $8k+7$ の形になろうと思えば，$7 \equiv 4+1+1+1 \pmod 8$ の形より短くすることはできない． □

§4　3 つの平方数の和

定理 3.8.　n **が 3 つ以下の平方数の和に書けない** $\Longleftrightarrow$ $n = 4^t(8k+7)$, $t,k \in \mathbb{Z}_{\geqq 0}$ **と書ける．**

証明. $\Longleftarrow$：$n = 4^t(8k+7)$ が $x^2+y^2+z^2$ と書けたとする．$t > 0$ なら，x, y, z はすべて偶数でなければならない．だから，

$$\frac{n}{4} = 4^{t-1}(8k+7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

となる．これを繰り返せば，$8k+7$ が 3 つの平方数の和に書けることになり，前節の命題 3.7 に矛盾する．

$\Longrightarrow$：この証明には初等的で簡単なものが知られていないので省略する．整係数の 3 変数の 2 次形式の議論が必要になる．たとえば日本語の本では，J.P. セール『数論講義』には，有理係数の 2 次形式の一般的議論を使っての証明があるが，高度な概念を必要とする．

直接整係数でやろうとすると，どうしても議論が長くなる (例えば，ローズ『数論教程』第 9 章参照).『ガウス整数論』(1801) 第 5 章には原形の証明がある．鍵になる概念は 2 次形式の判別式である． □

§5　ラグランジュの定理の証明

定理 3.9 (ラグランジュ). $g(2) \leqq 4$ **，つまり，すべての自然数** n **は 4 つの平方数の和に書ける．**

証明. $1 = 1^2+0^2+0^2+0^2$, $2 = 1^2+1^2+0^2+0^2$ と積公式 (Q4) から，すべての奇素数 p に対して示せばよいことがわかる．

p を奇素数とする．$(p-1)/2$ は整数である．そこで，2 つの集合

$$S = \left\{x^2 \mid x = 0, 1, 2, \cdots, \frac{p-1}{2}\right\},$$

$$T = \left\{-1-y^2 \mid y = 0, 1, 2, \cdots, \frac{p-1}{2}\right\}$$

を考えると，もちろん $S \cap T = \emptyset$ である．また，S の元には mod$p$ で考えたときも合同なものはない．というのは，もし $x^2 \equiv z^2 \pmod p$, $0 \leqq x, z \leqq (p-1)/2$ とすると，$p|x^2-z^2$，つまり $p|(x-z)(x+z)$ となり，

$p \nmid x+z$ だから，$p | x-z$ となるが，こうなり得るのは $x-z=0$ のときだけである．

同様にして，T の元の中にも，$\bmod p$ で合同なものはない．しかし，$|S| = |T| = 1 + \dfrac{p-1}{2} = \dfrac{p+1}{2}$ で，$|S \cup T| = p+1$ となり，$\bmod p$ での合同類は p 個しかないので，ある x, y が存在して

$$x^2 \equiv -1 - y^2 \pmod p, \quad 0 \leqq x, y \leqq \frac{p-1}{2}$$

となっている．これはまた，

$$x^2 + y^2 + 1^2 + 0^2 \equiv 0 \pmod p$$

であり，つまり，ある $k > 0$ に対して

$$(*) \qquad x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$$

が，$0 \leqq x_i \leqq (p-1)/2$ の範囲で整数解をもつことを意味している．また，$k < p$ であることもわかる．というのは $0 \leqq kp = \sum x_i^2 \leqq 4 \cdot \left(\dfrac{p-1}{2}\right)^2 = (p-1)^2 < p^2$ となるから．

さて，これで無限降下法 (定理 1.6) の第 1 段階が得られたことになる．$(*)$ で $k=1$ であればことは終っている．$k>1$ として，より小さな $0 < k' < k$ に対して $(*)$ が整数解をもつことを示せばよい．

場合 1. k **が偶数の場合．** 等式 $(*)$ から，x_i は，1) すべて奇数，2) すべて偶数，3) 2 つが偶数で，2 つが奇数，の 3 つの場合があるが，適当に変数の番号を付け替えてやれば，

$$\frac{x_1+x_2}{2}, \quad \frac{x_1-x_2}{2}, \quad \frac{x_3+x_4}{2}, \quad \frac{x_3-x_4}{2}$$

がすべて整数となり，

$$\left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 = \frac{k}{2}p$$

は，$k' = k/2 < k$ に対する方程式 $(*)$ が整数解をもつことを意味している．

場合 2.　k **が奇数の場合．** y_i を $y_i \equiv x_i \pmod k$ で，絶対値最小のものとする（$|y_i| < \dfrac{k}{2}$ となっている）．すると，

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod k$$

となって，

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = kk' \qquad (k' > 0)$$

となっている．ここで，$k' < k$ となっている．実際，$kk' = \sum y_i^2 < 4 \cdot \left(\dfrac{k}{2}\right)^2 = k^2$ だから．

そこで，この x_i と y_i に対して式 (Q4z) で定めた z_i を考えると，すべての i に対して $z_i \equiv 0 \pmod k$ であること，つまり $k|z_i$ であることがわかる．すると，

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = \left(\sum_{i=1}^{4} x_i^2\right)\left(\sum_{i=1}^{4} y_i^2\right) = (kp)(kk') = k^2k'p$$

であり，

$$\sum_{i=1}^{4}\left(\frac{z_i}{k}\right)^2 = \frac{1}{k^2}\left(\sum_{i=1}^{4} z_i^2\right) = \frac{k^2k'p}{k^2} = k'p$$

となって，無限降下法の第 2 段階が示されたことになる．したがって $k=1$ に対して方程式 $(*)$ が整数解をもつことになる．　□

§5.1　定理 3.8 を使う証明

定理 3.8 が証明してあるのなら，ラグランジュの定理 3.9 の別証明が容易に得られることをガウスが注意している．

任意の自然数 n は，$n = 4^t m$，$(t, m \in \mathbb{Z},\ t \geqq 0,\ m \geqq 1,\ m \not\equiv 0 \pmod 4)$ と表わされる．

$m \not\equiv 0 \pmod 4$ が 4 平方の和に書けることを示せばよい．もし，m が

$m = \sum_{i=1}^{4} a_i^2$ と書けているなら，$n = \sum_{i=1}^{4} (2^t a_i)^2$ と書けるから．

定理 3.8 によって，$m \equiv 1, 2 \pmod 4$ のときは，3 つの平方数の和に書ける．$m \equiv 3 \pmod 4$ のときは $l = m - (2a+1)^2 > 0$ を考えると，$l \equiv 2 \pmod 4$ になり，3 つの平方数の和に書ける． □

§5.2　$G(2) = g(2) = 4$ について

これまでに，$G(2) \geqq 4$ と $g(2) \leqq 4$ が示されている．

定義によって一般に，$G(k) \leqq g(k)$ であることが分かっているので，$4 \leqq G(2) \leqq g(2) \leqq 4$ となる． □

§6　5 つの正の整数の平方の和に表わされる整数

定理 3.10.　**1,2,3,4,6,7,9,10,12,15,18,33 以外の正の整数は，5 つの正の整数の平方の和に表わされる．**

証明.　$n > 169$ とする．ラグランジュの定理 3.8 ($g(2) = 4$) によって，$n - 169 = a_1^2 + a_2^2 + a_3^2 + a_4^2$, $a_i \geqq 0$ と表わすことができる．あとは，a_i のうちで 0 になるものの個数が 0, 1, 2, 3 であるのに応じて，169 の平方数の和による表示 $169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 10^2 + 8^2 + 2^2 + 1^2$ を使えばよい．

$1 \leqq n \leqq 169$ に対しては，直接計算によって，1,2,3,4,6,7,9,10,12,15,18,33 は 5 つの正の整数の平方の和に表わされ得ず (その数より小さい平方を調べればすぐに分かる)，それ以外は，5 つの正の整数の平方の和に表わされることを示す．具体的計算をここに上げるのは煩雑にすぎるので読者にゆだねることにする．

ちなみに，169 は例えば $169 = 11^2 + 6^2 + 2^2 + 2^2 + 2^2$ と書ける． □

§7 $g(3)$ について

3 次の場合にも同じようにしようとすれば，(Q2), (Q4) や 4 乗数のときの (Q24)(§8 参照) のような型の等式が欲しくなるが，成り立つと思った式がじつは間違っていたというような失敗の歴史がある．

1895 年に E. メレは

$$(\mathrm{Q23}) \qquad 6a(a^2 + x_1^2 + x_2^2 + x_3^2) = \sum_{i=1}^{3} \{(a + x_i)^3 + (a - x_i)^3\}$$

を使って，$g(3) \leqq 21$ であることを示した[6]．

ヤコビの示唆で，1835 年に A.R. ツァルノフ (Zarnow) という計算家が 3000 までの数を表わすのに必要な 3 乗数の最小値を計算した．23 以外は $\leqq 8$ 個，> 454 なら $\leqq 7$ 個，> 2183 なら $\leqq 6$ 個という結果だったが，9 個必要な 239 を見落としていた．1851 年に Z. ダーゼ (Dase) が間違いを正し，12000 までの表を作った．それによれば，7 つ必要な最大の数は 8042 であり，8 つ必要な必要な最大の数は 454 であり，8 個必要なものも 15 個しかない．それが 15, 22, 50, 114, 167, 175, 186, 212, 213, 238, 303, 364, 420, 428, 454 である．

1939 年にディクソンは $23 = 2 \times 2^3 + 7 \times 1^3$ と $239 = 5^3 + 3 \times 3^3 + 4 \times 2^3 + 1$ 以外の整数はすべて 8 個で書けることを示している．

§8 $g(4) \leqq 50$ の証明

まず，4 乗数とはどんなものかを思い出しておこう．

---

[6] ちなみにメレは 1907 年に $g(8)$ が有限であることを示している．

$$1^4=1,\ 2^4=16,\ 3^4=81,\ 4^4=256,\ 5^4=625,\ 6^4=1296,$$

$$7^4=2401,\ 8^4=4096,\ 9^4=6561,\ 10^4=10000$$

である．かなりまばらで，すべての数を表わそうとすればたくさんの数が必要な感じがするだろう．

少し具体的な計算をすることにより，$g(4)$ の下からの評価が得られる．

$15=15\cdot 1^4$,　$31=16+15=2^4+15\cdot 1^4$,　$47=16+16+15=2^4+2^4+15\cdot 1^4$,　$63=16+16+16+15=3\cdot 2^4+15\cdot 2^4$,　$79=16+16+16+16+15=4\cdot 2^4+15\cdot 2^4$ であることから，$g(4)\geqq 19$ であることがわかる．

上からの評価としては，任意の自然数が 50 個以下の 4 乗数の和に書けるということが初等的に証明できる．これを紹介することにする．

積公式 (Q2), (Q4) に類似な公式

(Q24)
$$6(x_1^2+x_2^2+x_3^2+x_4^2)^2=\sum_{1\leqq i<j\leqq 4}\{(x_i+x_j)^4+(x_i-x_j)^4\}$$

を使う．この式自身は，右辺の和の各項が $2(x_i^2+6x_ix_j+x_j^2)$ となることから分かる．また右辺は $12=2\times 6$ 項の 4 乗数の和で表わされている．

さて，任意の自然数 n を 6 で割ると，$n=6x+y$, $x\geqq 0$, $0\leqq y\leqq 5$ と書ける．ラグランジュの定理により，x を 4 つの平方数の和 $x=\sum_{i=1}^{4}x_i^2$ に書き，さらに各 x_i を 4 つの平方数の和

$$x_i=\sum_{j=1}^{4}x_{ij}^2,\quad (1\leqq j\leqq 4, 1\leqq i\leqq 4)$$

と書くと，

$$6x=6\sum_{i=1}^{4}\left(\sum_{j=1}^{4}x_{ij}^2\right)^2=\sum_{i=1}^{4}6\left(\sum_{j=1}^{4}x_{ij}^2\right)^2$$

は，$4\times 12=48$ 個の 4 乗数の和に書け，$y=y\cdot 1=y\cdot 1^4$ は $y(\leqq 5)$ 個の

4 乗数の和に書けるのだから，n は $48+5=53$ 個以下の 4 乗数の和に書けることになり，$g(4) \leqq 53$ が得られる．

これが，リウヴィルの与えた最初の $g(4)$ の評価である．

y について一律に評価するのでなく，少し工夫することにより，$g(4) \leqq 50$ であることを示すことができる．

$y=3,4,5$ のときだけが問題であるが，

$$6x+3=6(x-13)+3^4,\ 6x+4=6(x-2)+2^4,\ 6x+5=6(x-2)+2^4+1^4$$

を使えばよい．ここで，$n \leqq 50$ なら明らかに，50 個以下の $1=1^4$ で書けることに注意すると，$x-13<0$ となる $6\cdot 8+3=48+3=51$, $6\cdot 9+3=54+3=57$, $6\cdot 10+3=63$, $6\cdot 11+3=69$, $6\cdot 12+3=75$ は上の議論の適用外であるので，個別に処理する必要がある．

そのときは，$51=3\times 16+3\times 1$, $57=3\times 16+9\times 1$, $63=3\times 16+15\times 1, 69=4\times 16+5\times 1, 75=4\times 16+11\times 1$ と書けることに注意してもよいし，適当に 16 引いてもよい．□

§9　n 角数について

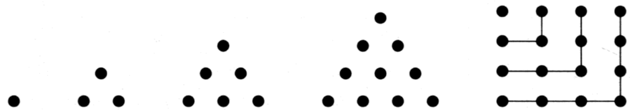
三角数 $1,3,6,\ldots$ はピュタゴラスの頃から知られており，下図のように黒丸点で三角形の形を作ったときの点の数で，1 辺が k のときの三角数を t_k とすると，

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
t_k	1	3	6	10	15	21	28	36	45	55	66	78	91	105	120

などとなる．定義自体が，数列 $\{t_k \mid k \geqq 1\}$ の階差数列が $t_k - t_{k-1} = k$ と公差 1 の等差数列であることを意味しているので，

$$t_k = 1+2+3+\ldots+k = \frac{k(k+1)}{2} = \binom{k}{2} \qquad (\text{t.1})$$

となる．



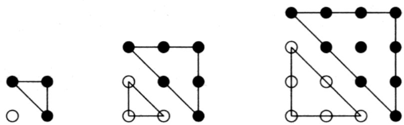
同じことを四角形で行えば四角数 $q_k = k^2$ が得られ，帰納的に

$$q_1 = 1,\ q_2 = q_1 + 3,\ q_3 = q_2 + 5,\ q_4 = q_3 + 7, \ldots,\ q_k = q_{k-1} + 2k - 1$$

と，つまり，最初の k 個の奇数の和 $q_k = \sum_{i=1}^{k}(2i-1)$ としても得られる (上図の 1 番右の図参照)．四角形を対角線で切り分けて得られる公式

$$q_k = t_k + t_{k-1}\ ;\ k^2 = \frac{k(k+1)}{2} + \frac{(k-1)k}{2} \qquad (\mathrm{t}.2)$$

は古代ギリシャから知られていた (ニコマコス，紀元 100 年頃)．当時はむしろこの式から，t_k の値を知ったのである．



同様に，公式

$$8t_k + 1 = q_{2k+1}\ ;\ 8\frac{k(k+1)}{2} + 1 = (2k+1)^2 \qquad (\mathrm{t}.3)$$

もまた幾何的に，長さ k の三角形を 2 つ合わせて，$k \times (k+1)$ の長方形を作り，これを 4 つ組合わせると長さ $2k+1$ の正方形から中心の点が 1 つ抜けたものが得られることから知られていた．

また，n 角形の辺の長さを増やしていくという定義から，p_k^n の (k に関する) 階差数列が初項 1 で公差が $n-2$ の等差数列になり，帰納的に，

$$p_1^n = 1, \quad p_k^n = p_{k-1}^n + (n-2)(k-1) + 1 \quad (k \geqq 2) \qquad (\mathrm{t}.4)$$

と定義されている．この定義にしたがって計算をしてみると次のような表が得られる．

k	1	2	3	4	5	6	7	8	9	10
$p_k^3 = t_k$	1	3	6	10	15	21	28	36	45	55
$p_k^4 = q_k$	1	4	9	16	25	36	49	64	81	100
p_k^5	1	5	12	22	35	51	70	92	117	145
p_k^6	1	6	15	28	45	66	91	120	153	190
p_k^7	1	7	18	34	55	81	112	148	189	235

さて，n 角形に対して同様にして得られる n 角数 p_k^n は，n 角形を隣り合う 2 辺とその両端を結んだ辺で切り分ければ，辺の長さ k の $n-1$ 角形と辺の長さが $k-1$ の三角形に分かれるので，

$$p_k^n = p_k^{n-1} + p_{k-1}^3 = p_k^{n-1} + t_{k-1} \qquad \text{(t.5)}$$

を満たすことが分かる．これを上の表で確かめてみて欲しい．

n 角数[7]の定義式 (t.4) から，数学的帰納法によって，

$$p_k^n = \frac{k((n-2)k-n+4)}{2} = \frac{k(k-1)}{2}(n-2) + k \qquad \text{(t.6)}$$

であることを示すのは難しくない．何角数であっても辺の数 k に関して 2 次式になっていることに注意する．

ディオファントス (紀元 250 年頃) は，(t.3) 式を得た議論の拡張として，かなり面倒ではあるが幾何学的議論だけで，これと同値な

$$8(n-2)p_k^n + (n-4)^2 = \{(n-2)(2k-1)+2\}^2 \qquad \text{(t.6}'\text{)}$$

を示しているという．

(t.6) 式で，n に値を入れて，

$$p_k^3 = t_k,\ p_k^4 = q_k,\ p_k^5 = \frac{k(3k-1)}{2},\ p_k^6 = k(2k-1),\ p_k^7 = \frac{k(5k-3)}{2}$$

とすれば，表の値を確かめることはやさしい．

また，上の表の各列を上から下に見てみると，初項 k の等差数列になっ

[7]これらを総称して，**多角数**とか**図形数**と言うこともある．

ており，しかも公差が t_{k-1} であることに気づく．これも，(t.6) 式を n のベキでまとめ直して

$$p_k^n = \frac{k(k-1)}{2}n + k(2-k) = t_{k-1}n + k(2-k) \tag{t.6$''$}$$

とすれば，確認される．

次に，数 p を与えたとき，n 角数になるだろうかということも考えられてきた．これは，与えられた数 p に対して，$n, k \in \mathbb{Z}$, $n \geqq 3$, $k \geqq 1$ に関する方程式

$$p_k^n = \frac{k((n-2)(k-1)+2)}{2} = p$$

を解くという問題になる．$p_1^n = 1$, $p_2^n = n$ であるから，$k \geqq 3$ として考えることにする．

まず，この式を変形して，整数 $n-2$ を表わした式

$$n - 2 = \frac{1}{k-1}\left(\frac{2p}{k} - 2\right) = \frac{2(p-k)}{k(k-1)}$$

の右辺が $\geqq 1$ であるという不等式を，k に関する 2 次不等式と見ると

$$k^2 + k - 2p \leqq 0$$

となり，これから

$$k \leqq \frac{1}{2}\left(\sqrt{8p+1} - 1\right)$$

が得られる．例えば，$p = 36$ であれば，$k \leqq (\sqrt{289} - 1)/2 = (17-1)/2 = 8$ となる．方程式は

$$72 = k(2 + (n-2)(k-1))$$

なので，$k|72$ であり，k の候補は $k = 2, 3, 4, 6, 8$ となる．これを上の式に代入にして，n が 3 以上の整数になる場合を求めてみると，$k = 4$ だけが除外されて，

$$36 = p_2^{36} = p_3^{13} = p_6^4 = p_8^3$$

となる．

§9.1　三角数の和

例えば，19 は $19 = 1 + 3 + 15 (= t_1 + t_2 + t_5) = 3 + 6 + 10 (= t_2 + t_3 + t_4)$ というように 3 つの三角数の和には書けるが，2 つの三角数の和には書けない．

定理 3.11.　**自然数 n が 2 つ以下の三角数の和に書ける $\Leftrightarrow$ $4n + 1$ の素因数で mod4 で 3 であるものは偶数ベキになっている．**

証明.　$n = t_j + t_k$ と書けたとすると，$2n = j(j + 1) + k(k + 1)$ であり，少し変形すると

$$2(4n + 1) = (2j + 1)^2 + (2k + 1)^2$$

となる．左辺は偶数で，平方の和に表わすとき，偶数の平方の和に表わせないことはすぐに分かる．したがって，$2(4n + 1)$ が 2 つの平方の和に書けるための条件を満たせばよいが，その条件 (定理 3.6) を見れば，$4n + 1$ の素因数に関する定理の条件になることが分かる．　□

定理 3.12.　**任意の自然数は 3 つ以下の三角数の和に書ける．**

証明.　任意の自然数 $n \in \mathbb{N}$ が 3 つの三角数の和に書ける，つまり，

$$n = t_x + t_y + t_z = \frac{x(x + 1)}{2} + \frac{y(y + 1)}{2} + \frac{z(z + 1)}{2}$$

と書けるとする．両辺に 8 を掛けて，右辺の各項を完全平方にすると

$$8n + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2$$

となる．

定理 3.8 によって，$8n + 3$ の形の整数は 3 つの平方の和に書ける．また，その 3 つの整数はすべて奇数でないといけないことも分かる．何故なら，偶

数^2 + 偶数^2 + 奇数^2 であれば $\equiv 3 \pmod 8$ とはなれない. □

これがガウス (1801) にある証明である. 4 角数に対する対応する定理はラグランジュの定理 3.9 そのものであるが, まったく同じ原理から与えたガウスの証明は §5.1 で与えておいた.

その当時, $n \geqq 5$ に対する, 高々 n 個の n 角数の和で自然数を分解するという問題は未解決で, その証明には何かしら別の原理が必要ではないかと, ガウスは述べている. その後, この問題は 1813 年に A.L. コーシーによって解かれた[8]. その証明によれば, 4 つ以外の n 角数の係数は 0 か 1 であるような和として表わせることがわかる. 確かに (t.6) 式でわかるように n 角数 p_k^n は k に関する 2 次式であり, それを思えば後は簡単な組合わせの議論だけなのかもしれない. 1816 年の『整数論』第 2 版の補遺の中で, ルジャンドルはこの証明を簡易化して, コーシーが仮定した $n = 3$ の場合の結果を仮定せずに証明を与えている.

§10 ウェアリングの問題

ヒルベルトが 1909 年にウェアリングの問題を解く, つまり, すべての $n \geqq 2$ に対して, $g(n)$ が有限であることを示す, までには実に色々な試みがなされていた[9]. それはすべて, $g(n)$ の上界を具体的に定めようという努力の延長線上にあった. $g(2) \leqq 4$ を示すラグランジュの証明, $g(3) \leqq 21$ を示すメレの証明, $g(4) \leqq 53$ を示すリウヴィルの証明を典型として, それを一般化する形でなされていた.

A. フルヴィッツは 1908 年に, 一般の k に対する証明への示唆をした. もし, a, b, c, d に関する恒等式

[8] Mém. Sc. Math. et Phys. de l'Institut de France, (1), **14**, 1813-1815, p.177-220. また, コーシー全集の (2),VI, p.320-353 に再録されている.

[9] 解説から読み始めた読者は, 本文第 3 章 §1 とそこにある訳註の歴史的コメントを参照すること.

$$p(a^2+b^2+c^2+d^2)^k = \sum_{i=1}^{r} p_i(\alpha_i a + \beta_i b + \gamma_i c + \delta_i d)^{2k}$$

が，ある正の整数 $p, p_1, \ldots p_r$ と整数 $\alpha_1, \ldots, \delta_r$ に対して成り立つならば，

$$g(2k) \leqq g(k)(p_1 + \cdots + p_r) + p - 1$$

となることを示した．このとき，$g(k)$ が有限なら $g(2k)$ も有限になるわけである．そして，$k=2$, $p=5040$, $r=72$, $p_i=6$ $(1 \leqq i \leqq 12)$, $p_i = 60$ $(13 \leqq i \leqq 24)$, $p_i = 1$ $(25 \leqq i \leqq 72)$ を満たすある等式を示し，当時ヴィーフェリッヒによって知られたばかりの $g(4) \leqq 37$ を使って, $g(8) \leqq 36119$ を求めている．直後に I. シューアも同様の恒等式を見つけて，$g(10)$ が有限であることを示している．ヴィーフェリッヒはまた別の型の恒等式を見つけ，$g(5) \leqq 59$, $g(7) \leqq 3806$ を示している．

そしてその直後にヒルベルトの証明が出るのである．A. フルヴィッツが予想して示せなかった等式

$$(x_1 + \cdots + x_5)^m = \sum_h \rho_h (a_{1h}x_1 + \cdots + a_{5h}x_5)^{2m}$$

が，あらゆる m に対して存在する（$a_{ih} \in \mathbb{Z}$, $\rho_h \in \mathbb{Q}_{>0}$）ことが鍵ではあるが，その証明に 5 重積分を使っている（最初の論文では 25 重積分だったが）．このような整数の問題を，積分を使って証明するというのには，単なる発想の転換以上のものが必要で，ヒルベルトの才能が特別なものであることを物語っている．

その後同じ年に，F. ハウスドルフが指数関数を用いてヒルベルトの証明を改良し，その後も簡易化の試みがなされてきており，じつはエリッソン (1971) によるヒルベルトの証明の簡易化を紹介しようかとも思ったが，かなり高度な微積分を使う証明はやはり本書の範囲を越えていると思い断念した．興味を持った読者は読んで見られたい．初等的な証明は，本文第 3 章のものより簡易化されたものを知らない．

エリッソンの総合報告 (1971) までに知られていた $g(k)$ と $G(k)$ についてまとめると，

k	2	3	4	5	6	7	8	9	10
$g(k)$	4	9	$19 \sim 21$	37	73	143	279	548	1079
$G(k)$	4	$4 \sim 7$	16	$\leqq 23$	$\leqq 36$	$\leqq 52$	$\leqq 73$	$\leqq 99$	$\leqq 122$

となる．

ディクソン (1928-1939)，S.S. ピライ (1933-1940)，R.K. ルブグンデイ (1942)，I. ニーヴン (1944) らの研究により，$k \geqq 6$ での $g(k)$ の値はほぼ決まっていると言ってよい．

$k \geqq 6$ で $3^k - 2^k + 2 < (2^k - 1)\left[(3/2)^k\right]$ という条件を満たせば，

$$g(k) = \left[(3/2)^k\right] + 2^k - 2$$

である．問題はこの条件であるが，$6 \leqq k \leqq 200000$ に対しては成り立つことが確かめられている．その上，この条件を満たさない k が有限個しかないことも，K. マーラー (1957) によって確かめられているのだが，満たさない k の集合を定めることはできていない．$g(4)$ もある数 (値も知られている) 以上では 19 個で書けることがわかっているので，それ以下の数をすべて確かめればよく，原理的には定まることになっている．コンピュータの進歩によって，本書の出版以前に確定することすらあり得る．

$G(k)$ についても研究は進んでいる．$G(4) = 16$ は H. ダヴェンポート (1939) によって確定された．

ヴォーガン (1981) により，ハーディー-リトルウッドの方法が大きく改善されて，それを応用して，ブルーデルン (1990)，ウーリー，ヴォーガンらは $G(k)$ の評価を劇的に改善している．

k	5	6	7	8	9	10	11	12
$G(k)$	$\leqq 17$	$\leqq 24$	$\leqq 33$	$\leqq 42$	$\leqq 51$	$\leqq 59$	$\leqq 67$	$\leqq 76$
k	13	14	15	16	17	18	19	20
$G(k)$	$\leqq 84$	$\leqq 92$	$\leqq 100$	$\leqq 112$	$\leqq 120$	$\leqq 129$	$\leqq 138$	$\leqq 146$

は，1995 年での最善値であるが，その後もウーリーたちは精力的に研究しているので，値は次々と更新されているかも知れない．

大きい方の k に対しても，ウーリー (1992) は $G(k) \leqq (1 + o(1))k \log k$

という評価を与えている．もっと厳密に，$k \to \infty$ につれて

$$G(k) < k(\log k + \log\log k + O(1))$$

という評価が得られている[10]．第 3 章の初めの脚注にある $G(k)$ の評価の歴史から見ても劇的な進歩である．

§11　ゴールドバッハの問題

1 が素数でないので，いくつ以上のという言い方をするが，本文とは違うが，改めて $P = \{0\} \cup \mathbb{P}$ とおけば，ゴールドバッハがオイラーに送った予想は

$$\text{(G)} \qquad \mathbb{N} \subset (P + P + P) \cup \{1\}$$

と表現され，それと同値だというオイラーの言い換えは

$$\text{(G2)} \qquad 2\mathbb{N} \subset P + P$$

と書かれる．

この同値性を確かめよう．

(G) $\Longleftarrow$ (G2)：3 以上の奇数だけを表わせばよい．それは $2n+1$ $(n \geqq 1)$ と表わされる．$2n-2 \in 2\mathbb{N}$ なので，(G2) により，$2n-2 = p+p'$, $p, p' \in P$ と書ける．したがって，$2n+1 = 3+p+p'$ と書ける．

(G) $\Longrightarrow$ (G2)：偶数は $2n$ $(n \geqq 1)$ と表わされる．$2n+2 > 1$ なので，(G) により，$2n+2 = p+p'+p''$, $p, p', p'' \in P$ と書ける．左辺は偶数であり，右辺の素数はすべて奇数であることはできず，その 1 つ，たとえば p'' は偶数である素数，つまり 2 でなければならない．したがって，$2n = p+p'$ と書ける．□

[10] $o(1)$ や $O(1)$ は，ランダウの記号とよばれ，例えば $k \to \infty$ の時などの漸近挙動のオーダーを表わしている．今の場合，$O(1)$ は定数以下のオーダーの量で，$o(1)$ は定数より小さいオーダーの量であることを意味している．ただし，値自体は非常に大きい可能性があることに注意する．



ハーディ(左) とリトルウッド (右)

残念ながら，具体的な数でこの事実を確かめること以外に，初等的なアプローチは今のところない．研究の歴史を述べて許していただく．

1920 年代にハーディーとリトルウッドが精密な解析的手法を用いて研究するまで，ほとんど進展がなかった．ヴィノグラードフ (1937) が，十分大きな奇数，つまりある数 c 以上の奇数は 3 つの素数の和で書けることを示したときも，精密な指数関数値の級数の評価を用い，さらにディリクレの算術定理を使っている．その後，c の値も具体的に求まるようになり，$c \leqq 3^{3^{15}}$ (1956 年)，$c \leqq 10^{43000}$ (1989 年) までになったが，まだコンピュータで全数検査できる大きさではない．1980 年の時点では，10^8 までの数に対してコンピュータで確認されているが，現在ではいくつまでになっているだろうか．

この算術定理の応用として，エラトステネスのふるいの一般化である**ふるい法**がブルン (1919) によって開発され，十分大きな偶数は $P_9 + P_9$ の元であることが示された．ここで，P_k というのは高々 k 個の素数の積として表

わされる数 (k 概素数) のことである．

以降，この方向の研究は，セルバーグ (1950) が，十分大きな偶数は $P_2 + P_3$ の元であることを示した．また，1947 年にレニが，十分大きな偶数が $P_1 + P_k$ の元であるような k が存在することを示して以来，k を小さくする努力がなされてきたが，1966 年にチェン (1973/78) が $k = 2$ であることを示して以来の進展はない．またロス (1975) はチェンの定理の簡単な証明を与えているが，初等的とは言えず，ここでは紹介できない．

(G2) に対してもコンピュータでの検査は行われていて，1993 年で，4×10^{11} までには反例がないことが知られている．

(G2) については，密度 0 のある集合を除けば成り立つことが，T. エスターマン (1938)，J.G. ヴァン・デル・コルプト (1939)，N.G. チュダコフらによって独立に示された．

この予想に対するもう 1 つのアプローチが，すべての自然数をいくつかの素数の和に書くということである．その始まりがシュニレルマンの定理であって，その解説が本書の第 2 章であった．いくつの和に書けるかという数をシュニレルマン定数と言い，具体的な評価もなされている．

大きく分けて 3 つの方面からゴールドバッハの予想の攻略がなされているのだが，どれかが一番乗りをするのか，それともまったく別のアプローチが必要なのかわかっていない．

読者の中から，攻略に参加し成功する人が出ることを期待しつつ，解説を終わることにしよう．

数の表

本書，特に解説で与えた色々な定理を具体的な数で確かめることができるように，色々な数の表を挙げておく．また，定理を利用して，さらに色々な発見が得られるだろう．

遊び方の例を少し示しておこう．

1999 はどんな数か？

例えば，本書の原稿は 1999 年に完成していたのだが，その 1999 は，それ自身素数だが，$1999 = 5+997+997$ と 3 つの奇素数の和に書ける．$1999 \equiv 3 \pmod 4$ だから，2 つの平方数の和には書けず (定理 3.2)，さらに，$1999 \equiv 7 \pmod 8$ だから，3 つの平方数の和にも書けないが (定理 3.8)，例えば，$1999 = 4 + 25 + 36 + 1936 = 2^2 + 5^2 + 6^2 + 44^2$ と，4 つの平方数の和には書けている．

また，$1999 = 1 + 27 + 27 + 216 + 1728 = 1^3 + 3^3 + 3^3 + 6^3 + 12^3$ と，5 つの正の立方数の和に書け，$1999 = 1296 + 625 + 4 \times 16 + 16 + 16 + 16 + 16 + 14 \times 1 = 14 \times 1^4 + 4 \times 4^4 + 5^4 + 6^4$ と 20 個の 4 乗数の和とも，$1999 = 3 \times 625 + 81 + 2 \times 16 + 11 \times 1 = 11 \times 1^4 + 2 \times 2^4 + 3^4 + 3 \times 5^4$ と 17 個の 4 乗数の和とも書ける．もっと少ない数で書けるかも知れない．

また，$1999 = 1953 + 45 + 1 = t_{62} + t_9 + t_1$ と 3 つの三角数の和に書けるが，$4 \times 1999 + 1 = 7997 = 11 \times 727$ は mod 4 で 3 である 2 つの素因数の積になるので，1999 は 2 つの三角数の和には書けない (定理 3.11).

平方数の表

平方数の表はまた，素数の判定にも使える場合がある．例えば 10001 を考える．$10001 = 1 + 100^2$ だから，$4m+3$ 型の素因数はあっても平方の形で入っていることになるが (定理 3.6)，平方数の表を見ても，10001 の約数になるものはありそうにない．もし素数ならこのほかに平方数の和に書く方法はないことになるが (定理 3.5)，$10001 = 4225 + 5776 = 65^2 + 76^2$ となるので，合成数であることが分かる．実際には $10001 = 73 \times 137$ で，約数を実際に求めるのはやさしくないが．約数を計算しなくでも合成数であることが分かるところが面白い．

素数は 2 列の等差数列の中に

双子素数についてもこれまでに述べたことから，いくつかのことを実験してみることができる．ディリクレの算術定理 2.3 によって，$n \geqq 1$ に対して $6n \pm 1$ という数列にはそれぞれ無限個の素数が存在するし[11]，また 2 と 3 を除けば，他の形の素数はあり得ない．実際，

$$6n+2 = 2(3n+1), \quad 6n+3 = 3(2n+1), \quad 6n+4 = 2(3n+2)$$

である．そこで，$6n-1$ と $6n+1$ を並べて書いてみて，素数表で素数かどうかをチェックする．

$6n-1$	5	11	17	23	29	35	41	47	53	59	65	71	77	83	89	95	101	⋯
$6n+1$	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91	97	103	⋯

当たり前だが，素数表をたどっていくと，必ずこの 2 列の中に現れることが確かめられる．そして，上下ともに素数のときが双子素数を表わしている．こうした手作業はやってみると思いの外に面白いものである．

数表は数列

また，数表というものは数列の例でもある．数列があれば，数列の性質を知りたくなる．そのために階差数列をとってみるというのも 1 つの方法である．

[11] この場合だけなら定理 2.4 と同様に証明することができる．読者に残しておこう．

例えば，公差 d の等差数列 $a_n = a_0 + nd$ ならば，その階差数列 $b_n = a_{n+1} - a_n$ を考えれば，$b_n = d$ と定数になり，さらに階差をとれば，0 だけからなる数列になる．

$a_n = n^2$ ならば，$b_n = (n+1)^2 - n^2 = 2n+1$ であり，その階差は 2 だけからなる数列になる．

一般に，数列 $\{a_n\}$ に対して，k 次階差数列 a_n^k を，$a_n^0 = a_n$ かつ $a_n^k = a_{n+1}^{k-1} - a_n^{k-1}$ と定義すれば，n の k 次式で表わされる一般項 a_n をもつ数列の $k+1$ 次階差数列は 0 だけからなる，つまり $a_n^{k+1} = 0$ となることを示すことは容易である (数学的帰納法を使う)．これも，以下の表で具体的に確かめてみて欲しい．

$a_n = n^3$ なら，$a_n^4 = 0$ だが，では a_n^3 はどんな定数だろうか？　$k = 4$ でもやってみれば，$a_n = n^k$ の時の a_n^k がどうなるかは容易に想像がつくだろう．

a_n が n の多項式で表わされれば，このように単純な結論が得られるが，素数列 p_n に対してはどうなるだろうか．これにはまったく想像が働かない．やってみよう．するとすぐに，値が振動して負の値も出てくることがわかる．そこで，階差数列からの再現性はなくなるが，絶対階差数列 $p_n^k = |p_{n+1}^{k-1} - p_n^{k-1}|$ を考えてみたらどうなるだろうか．n をある程度の長さ表示して，k を次々と動かして表示すると面白いアニメーションが見えることに気付く．先頭は常に 1，その後ろに 0 がいくつか並び，そのあとに 2 が来る．その 2 が段々前に進んで来て，先頭の 1 にぶつかって 1 になる．次々と 2 が進んで来ては消える．n が十分に長いと，2 が生まれる所も見える．$k \leqq 63418$ までなら確認されているが，この記録を破るためには，p_{63418} より先の素数表が必要になる．

このほかにもいろいろと楽しみ方があるだろう．面白い楽しみ方を考えついた人は訳者にも教えてほしい．できれば e-メールで．

§1　素数

10100 までの素数 (p_k は $k \leqq 1240$ 番目の素数) の表：

k の 1 の位	1	2	3	4	5	6	7	8	9	10
0+	2	3	5	7	11	13	17	19	23	29
10+	31	37	41	43	47	53	59	61	67	71
20+	73	79	83	89	97	101	103	107	109	113
30+	127	131	137	139	149	151	157	163	167	173
40+	179	181	191	193	197	199	211	223	227	229
50+	233	239	241	251	257	263	269	271	277	281
60+	283	293	307	311	313	317	331	337	347	349
70+	353	359	367	373	379	383	389	397	401	409
80+	419	421	431	433	439	443	449	457	461	463
90+	467	479	487	491	499	503	509	521	523	541
100+	547	557	563	569	571	577	587	593	599	601
110+	607	613	617	619	631	641	643	647	653	659
120+	661	673	677	683	691	701	709	719	727	733
130+	739	743	751	757	761	769	773	787	797	809
140+	811	821	823	827	829	839	853	857	859	863
150+	877	881	883	887	907	911	919	929	937	941
160+	947	953	967	971	977	983	991	997	1009	1013
170+	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
180+	1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
190+	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
200+	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
210+	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
220+	1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
230+	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
240+	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
250+	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
260+	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
270+	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
280+	1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
290+	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
300+	1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
310+	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
320+	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
330+	2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
340+	2293	2297	2309	2311	2333	2339	2341	2347	2351	2357

k の 1 の位	1	2	3	4	5	6	7	8	9	10
350+	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
360+	2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
370+	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
380+	2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
390+	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
400+	2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
410+	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
420+	2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
430+	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
440+	3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
450+	3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
460+	3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
470+	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
480+	3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
490+	3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
500+	3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
510+	3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
520+	3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
530+	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
540+	3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
550+	4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
560+	4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
570+	4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
580+	4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
590+	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
600+	4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
610+	4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
620+	4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
630+	4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
640+	4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
650+	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
660+	4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
670+	5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
680+	5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
690+	5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
700+	5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
710+	5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
720+	5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
730+	5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
740+	5641	5647	5651	5653	5657	5659	5669	5683	5689	5693

k の 1 の位	1	2	3	4	5	6	7	8	9	10
750+	5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
760+	5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
770+	5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
780+	5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
790+	6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
800+	6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
810+	6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
820+	6311	6317	6323	6329	6337	6343	6353	6359	6361	6367
830+	6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
840+	6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
850+	6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
860+	6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
870+	6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
880+	6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
890+	6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
900+	7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
910+	7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
920+	7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
930+	7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
940+	7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
950+	7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
960+	7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
970+	7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
980+	7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
990+	7841	7853	7867	7873	7877	7879	7883	7901	7907	7919
1000+	7927	7933	7937	7949	7951	7963	7993	8009	8011	8017
1010+	8039	8053	8059	8069	8081	8087	8089	8093	8101	8111
1020+	8117	8123	8147	8161	8167	8171	8179	8191	8209	8219
1030+	8221	8231	8233	8237	8243	8263	8269	8273	8287	8291
1040+	8293	8297	8311	8317	8329	8353	8363	8369	8377	8387
1050+	8389	8419	8423	8429	8431	8443	8447	8461	8467	8501
1060+	8513	8521	8527	8537	8539	8543	8563	8573	8581	8597
1070+	8599	8609	8623	8627	8629	8641	8647	8663	8669	8677
1080+	8681	8689	8693	8699	8707	8713	8719	8731	8737	8741
1090+	8747	8753	8761	8779	8783	8803	8807	8819	8821	8831
1100+	8837	8839	8849	8861	8863	8867	8887	8893	8923	8929
1110+	8933	8941	8951	8963	8969	8971	8999	9001	9007	9011
1120+	9013	9029	9041	9043	9049	9059	9067	9091	9103	9109
1130+	9127	9133	9137	9151	9157	9161	9173	9181	9187	9199
1140+	9203	9209	9221	9227	9239	9241	9257	9277	9281	9283

k の 1 の位	1	2	3	4	5	6	7	8	9	10
1150+	9293	9311	9319	9323	9337	9341	9343	9349	9371	9377
1160+	9391	9397	9403	9413	9419	9421	9431	9433	9437	9439
1170+	9461	9463	9467	9473	9479	9491	9497	9511	9521	9533
1180+	9539	9547	9551	9587	9601	9613	9619	9623	9629	9631
1190+	9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
1200+	9739	9743	9749	9767	9769	9781	9787	9791	9803	9811
1210+	9817	9829	9833	9839	9851	9857	9859	9871	9883	9887
1220+	9901	9907	9923	9929	9931	9941	9949	9967	9973	10007
1230+	10009	10037	10039	10061	10067	10069	10079	10091	10093	10099

http://www.utm.edu/research/primes/ftp/short.txt はインターネット上の素数に関するページで，いろいろな素数の表がテキストの形で掲載されている．

§2　平方数＝2 乗数＝四角数

平方数 $k^2 = q_k$ の 10000 までの表：

k の 1 の位	1	2	3	4	5	6	7	8	9	10
0+	1	4	9	16	25	36	49	64	81	100
10+	121	144	169	196	225	256	289	324	361	400
20+	441	484	529	576	625	676	729	784	841	900
30+	961	1024	1089	1156	1225	1296	1369	1444	1521	1600
40+	1681	1764	1849	1936	2025	2116	2209	2304	2401	2500
50+	2601	2704	2809	2916	3025	3136	3249	3364	3481	3600
60+	3721	3844	3969	4096	4225	4356	4489	4624	4761	4900
70+	5041	5184	5329	5476	5625	5776	5929	6084	6241	6400
80+	6561	6724	6889	7056	7225	7396	7569	7744	7921	8100
90+	8281	8464	8649	8836	9025	9216	9409	9604	9801	10000

§3　立方数=3 乗数

3 乗数 k^3 の 27000 までの表：

k	1	2	3	4	5	6	7	8	9	10
0+	1	8	27	64	125	216	343	512	729	1000
10+	1331	1728	2197	2744	3375	4096	4913	5832	6859	8000
20+	9261	10648	12167	13824	15625	17576	19683	21952	24389	27000

§4　4 乗数

4 乗数 k^3 の 10000 までの表：

k	1	2	3	4	5	6	7	8	9	10
k^4	1	16	81	256	625	1296	2401	4096	6561	10000

§5　三角数

三角数 $p_k^3 = t_k$ の 10000 までの表：

k の 1 の位	1	2	3	4	5	6	7	8	9	10
0+	1	3	6	10	15	21	28	36	45	55
10+	66	78	91	105	120	136	153	171	190	210
20+	231	253	276	300	325	351	378	406	435	465
30+	496	528	561	595	630	666	703	741	780	820
40+	861	903	946	990	1035	1081	1128	1176	1225	1275
50+	1326	1378	1431	1485	1540	1596	1653	1711	1770	1830
60+	1891	1953	2016	2080	2145	2211	2278	2346	2415	2485
70+	2556	2628	2701	2775	2850	1926	3003	3081	3160	3240
80+	3321	3403	3486	3570	3655	3741	3828	3916	4005	4095
90+	4186	4278	4371	4465	4560	4656	4753	4851	1950	5050
100+	5151	5253	5356	5460	5565	5671	5778	5886	5995	6105
110+	6216	6328	6441	6555	6670	6786	6903	7021	7140	7260
120+	7381	7503	7626	7750	7875	8001	8128	8256	8385	8515
130+	8646	8778	8911	9045	9180	9316	9453	9591	9730	9870

そして $t_{141} = 10011$ である.

§6　5 角数

5 角数 p_k^5 の表 ($1 \leqq k \leqq 90$)：

k	1	2	3	4	5	6	7	8	9	10
0+	1	5	12	22	35	51	70	92	117	145
10+	176	210	247	287	330	376	425	477	532	590
20+	651	715	782	852	925	1001	1080	1162	1247	1335
30+	1426	1520	1612	1717	1820	1926	2035	2147	2262	2380
40+	2501	2625	2752	2882	3015	3151	3290	3432	3577	3725
50+	3876	4030	4187	4347	4510	4676	4845	5017	5192	5370
60+	5551	5735	5922	6112	6305	6501	6700	6902	7107	7315
70+	7526	7740	7957	8177	8400	8626	8855	9087	9322	9560
80+	9801	10045	10292	10542	10795	11051	11310	11572	11837	12105

参考文献

[訳者注意]　文献表は原著にはない．手紙の形式の本文に，論文や教科書のような文献の引用は似合わないと思ったのだろう．現在の読者には，文献表がある方が便利だろうと思って，訳者が補った．

[アイグナー，ツィーグラー (1998)]　M.Aigner & G.M.Ziegler :『天書の証明』(*Proofs from the Book*), Springer, 1998, pp.199. シュプリンガー・フェアラーク東京から日本語訳が出版される予定．[p.114, p.128]

[アルティン，シェルク (1943)]　E.Artin & P.Scherk :『整数の 2 つの集合の和について』(*On the Sum of Two Sets of Integers*), Annals of Math., **44** (1943), 138-142. [p.30]

[ヴァン・デル・コルプト (1939)]　J.G.van der Corput :『素数と素数の 2 乗の和について』(*Über Summen von Primzahlen und Prim-zahlquadraten*), Math. Ann., **116** (1939), p.1-50. [p.148]

[ヴィノグラードフ (1935)]　I.M.Vinogradov :『ウェアリングの問題について』(*On Waring's Problem*), Ann. of Math. **36** (1935), 395-405. [p.44]

[ヴィノグラードフ (1937)]　——：『奇数を 3 つの素数の和に表わすこと』(*Representation of an odd number as the sum of three primes*), Dokl.Akad.Nauk, USSR, **15** (1937), 169-172 (ロシア語). [p.20, p.147]

[ヴィノグラードフ (1959)]　——：『$G(n)$ の上界について』(*On an upper bound for* $G(n)$), Izv.Akad.Nauk, USSR, **23** (1959), 637-642. [p.44]

[ヴィーフェリッヒ (1909)]　A.Wieferich :『あらゆる整数が高々9 つの立方数の和で表わされるという定理の証明』(*Beweis des Satses, daß eine jede ganze Zahl als Summe von höchstens neun Kuben darstellun läßt*), Math. Ann. **66** (1909), p.95-101. [p.43]

[ヴィーフェリッヒ (1909a)]　A.Wieferich :『整数を 4 乗数の和に表わすことについて』(*Über die Darstellung der Zahlen als Summen von Biquadraten*), Math. Ann. **66** (1909), p.106-108. [p.43]

[ウェアリング (1770)]　E.Waring :『代数学の考察』(*Meditationes algebraicae*), 1770.　ゴールドバッハの予想が初めて印刷されたこのも本書．[p.43]

[ヴォーガン (1981)]　R.C.Vaughan :『ハーディー・リトルウッドの方法』(*The Hardy-Littlewood Method*), Cambridge Univ.Press, Cambridge(1981). [p.145]

[ヴォーガン (1989)]　R.C.Vaughan :『ベキの小さなウェアリングの問題につい

て』(*On Waring's problem for smaller exponets*), Proc. London Math. Soc., (3) **39** (1989), p.445-463. [p.145]

[ヴォーガン，ウーリー (1993)]　R.C.Vaughan & T.D.Wooley :『ウェアリングの問題の更なる改善 III : 8 次』(*Further improvements in Waring's problem, III: eighth powers*), Philos. Trans. Roy. Soc. London Ser. A **345** (1993), 385-396. [p.145]

[ヴォーガン，ウーリー (1994)]　R.C.Vaughan & T.D.Wooley :『ウェアリングの問題の更なる改善』(*Further improvements in Waring's problem*), Acta Math. **174** (1995), 147-240. [p.145]

[ウーリー (1992)]　Trevor D.Wooley :『ウェアリングの問題の大きな改善』(*Large improvements in Waring's problem*), Ann. of Math., **135** (1992), p.131-164. [p.145]

[エスターマン (1938)]　T.Estermann :『ほとんどすべての偶数が 2 つの素数の和であることの証明』(*Proof that almost all even positive integers are sum of two primes*), Proc. London Math. Soc., **44** (1938), p.307-314. [p.148]

[エリッソン (1971)]　W.J.Ellison :『ウェアリングの問題』(*Waring's Problem*), Amer.Math. Monthly, **78** (1971), p.10-36. [p.xix, p.44, p.144]

[エルデシュ(1930)]　P.Erdös :『チェビシェフの定理の証明』(*Beweis eines Satzes von Tschebyshef*), Acta Sci. Math.(Szeged) **5** (1930-32), 194-198. [p.117]

[エルデシュ(1949)]　—— :『素数定理の初等的な証明に導く初等整数論の新しい方法について』(*On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*), Proc. Nat. Acad. Sci. U.S.A., **35** (1949), p.374-384. [p.115]

[ガウス (1801)]　C.F.Gauß :『ガウス整数論』(高瀬正仁訳) 数学史叢書，朝倉書店 (1995). 原著は *Disquisitiones Arithmeticae*, 1801. [p.xix, p.132, p.143]

[クーラント，フルヴィッツ (1964)]　A.Hurwitz & R.Courant :『楕円関数論』(足立恒男＋小松啓一訳) シュプリンガー数学クラシックス (1991). 原著は *Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen*, 第 4 版, Springer, 1964. 初版 (1922), 第 2 版 (1925), 第 3 版 (1929). [p.18]

[ケンプナー (1912)]　A.J.Kempner :『ウェアリングの問題と 1 つの一般化について』(*Über das Waringsche Problem und einige Verallgemeinerungen*), Inaugural-Dissertation, Göttingen, 1912. [p.44]

[ゴールドマン (1998)]　J.R.Goldman :『数学の女王：歴史的な動機での数論ガイド』(*The Queen of Mathematics: A Historically Motivated Guide to Number Theory*), A.K.Peters, Wellesley, 1998, pp.525. [p.xix]

[ザギエ (1990)]　Don Zagier :『あらゆる素数 $p \equiv 1 \pmod 4$ が 2 つの平方数の

和であることの 1 文の証明』(*A One-Sentence Proof That Every Prime* $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares*), Amer.Math. Monthly, **97** (1990), p.144. [p.128]

[シュニレルマン (1930)]　L.G.Shnirelman :『数の加法的性質について』(*Über additive Eigenshaften von Zahlen*), Ann. Inst. Polytech. Novocherkask, **14** (1930), 3-28. と Math. Ann., **107** (1933), 649-690. [p.27]

[セール (1970)]　J.P.Serre :『数論講義』(彌永健一訳) 岩波書店 (1979). 原著は *Cours d'Arithmetique*, Presses Universitaires de France (1970). [p.132]

[セルバーグ (1949)]　A.Selberg :『素数定理の初等的証明』(*An elementary proof of the prime number theorem*), Annals of Math., **50** (1949), p.305-313. [p.115]

[セルバーグ (1950)]　A.Selberg :『一般ふるい法と素数理論におけるその位置』(*The general sieve method and its place in prime number theory*), Proc. ICM, Cambridge, 1950. [p.148]

[ダヴェンポート (1939)]　H.Davenport :『4 次のウェアリングの問題』(*On Waring's problem for four powers*), Ann. of Math., **40** (1939), p.731-747. [p.145]

[チェン (1958)]　J.-R. Chen(陳景潤) :『n 乗数に対するウェアリングの問題について』(*On Waring's problem for nth powers*), Acta. Math. Sinica, **8** (1958), 英訳は Chinese Math. Acta, 8(1967), 849-853. [p.44]

[チェン (1964)]　—— :『$g(5)$ に対するウェアリングの問題』(*Waring's problem for* $g(5)$), Sci. Sinica, **13** (1964), 1547-1568. [p.44]

[チェン (1973/78)]　—— :『大きな偶数を素数と高々2つの素数の積との和として表わすことについて. I, II』(*On the representation of a large even number as the sum of a prime and the product of at most two primes, I and II*), Sci. Sinica, **16** (1973), 157-176(I), **21** (1978), 421-430(II). [p.121, p.148]

[ディクソン (1919-23)]　L.E.Dickson :『数論の歴史　全 3 巻』(*History of the Theory of Number*), Carnegie Institution, Washington D.C., 1919-23. Chelsea から復刻版 (1952). [p.xix]

[ディクソン (1939)]　L.E.Dickson :『23 と 239 以外のすべての整数は 8 つの立方数の和である』(*All integers except 23 and 239 are sums of 8 cubes*), Bull. Amer. Math. Soc. (1934) 631-640. [p.136]

[トス (1998)]　G.Toth :『数学名所案内　上下』(蟹江幸博訳) シュプリンガー・フェアラーク東京 (1999,2000). 原著は *Glimpses of Algebra and Geometry*, Springer-Verlag New York (1998). [p.82]

[ナゲル (1964)]　T.Nagell :『数論入門』(*Introduction to Number Theory*), 第 2 版, Chelsea, New York, 1964. [p.xix]

[ハイラー, ワナー (1997)]　E.Hairer & G.Wanner :『解析教程　上下』(蟹江幸

博訳) シュプリンガー・フェアラーク東京 (1997). 原著は *Analysis by Its History*, Springer-Verlag (1995). [p.105, p.114]

[ハーディー, ライト (1979)] G.H.Hardy & E.M.Wright :『数論入門 第5版』(*An Introduction to the Theory of Numbers*), Oxford Science Publications, 1979, pp.426. 初版 (1938), 第2版 (1945), 第3版 (1954), 第4版 (1960), 第5版 (1979). [p.xix]

[ハーディー, リトルウッド (1920)] G.H.Hardy & J.E.Littlewood :『ウェアリングの問題の新しい解答』(*A New Solution of Waring's Problem*), Quartely Journal of Math., **48** (1920), p.272-293. [p.44, p.147]

[ハーディー, リトルウッド (1920a)] —— :『「数の分割」の諸問題 I : ウェアリングの問題の新しい解答』(*Some Problems of 'Partitio Numerorum':I. A New Solution of Waring's Problem*), Nachrichten von der K.Gesellshaften zu Götingen, Math.-phys. Klasse, 1920, p.33-54. [p.44, p.147]

[ハーディー, リトルウッド (1920b)] —— :『「数の分割」の諸問題 II : あらゆる大きな数は高々21個の4乗数の和であることの証明』(*Problems of 'Partitio Numerorum':II. Proof that every large number is the sum of at most 21 biquadrates*), Math.Zeitshrift, **9** (1921), p.14-27. [p.44, p.147]

[ハーディー, リトルウッド (1922)] —— :『「数の分割」の諸問題 IV : ウェアリングの問題の特異級数と数 $G(k)$ の値』(*Problems of 'Partitio Numerorum':IV. The singular series in Waring's problem and the value of the number* $G(k)$), Math.Zeitshrift, **12** (1922), p.161-188. [p.44, p.147]

[ハーディー, リトルウッド (1925)] ——:『「数の分割」の諸問題 VI : ウェアリングの問題の研究の続き』(*Problems of 'Partitio Numerorum':VI. Further researches in Waring's problem*), Math.Zeitshrift, **23** (1925), p.1-37. [p.44, p.147]

[ハーディー, リトルウッド (1928)] —— :『「数の分割」の諸問題 VIII : ウェアリングの問題の数 $\Gamma(k)$』(*Problems of 'Partitio Numerorum':VIII. The number* $\Gamma(k)$ *in Waring's problem*), Proc. of the London Math. Soc., (2) **28** (1928), p.518-542. [p.44, p.147]

[ヒルベルト (1909)] D.Hilbert :『整数をある固定した数の n 乗数で表わすことができることの証明（ウェアリングの問題）』(*Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl* n*-ter Potenzen (Waringsches Problem)*), Math. Ann. **67** (1909), p.281-300. [p.43, p.143]

[ファン・デル・ヴェルデン (1927)] van der Waerden :『バウデット予想の証明』(*Beweis einer Baudetschen Vermutung*), Nieuw Arch. Wiskunde, **15** (1927), 212-216. [p.8]

[ファン・デル・ヴェルデン (1965)] van der Waerden :『バウデット予想の証明はいかにして発見されたか』(*Wie der Beweis der Vermutung von Baudet gefunden wurde*), Abh. Math. Sem. Univ. Hamburg, **28** (1965), 6-15.

英訳が *How the proof of Baudet conjecture was found*, Studies in Pure Math. (L.Mirsky 編), Academic Press (1971) にある．[p.8]

[ブルーデルン (1990)]　J.Brüdern ：『5 次のウェアリングの問題と関連した話題』(*On Waring's problem for fifth powers, and some related topics*), Proc. London Math. Soc., (3) **61** (1990), 457-179. [p.145]

[ブルン (1919)]　V.Brun :『エラトステネスのふるいとゴールドバッハの予想』(*Le crible d'Eratosthène et le théorème de Goldbach*), C.R. Acad.Sci. Paris, **168** (1919), 544-546. [p.122]

[ブルン (1919a)]　—— :『分母が「双子素数」である級数 $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ は収束するか有限級数である』(*La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ *où les dénominateurs sont "nombres premiers jummeaux" est convergente ou finie*), Bull.Sci.Math., (2) **43** (1919), 100-104 and 124-128. [p.121]

[ベイカー (1984)]　Alan Baker ：『初等整数論講義』(片山孝次訳) サイエンス社 (1992)．原著は *A Concise Introduction to the Theory of Numbers*), Cambridge Univ. Press(1984). [p.xix]

[ユーウェル (1998)]　J.A.Ewell :『三角数定理のトリオ』(*A Trio of Triangular Number Theorems*), Amer. Math. Monthly, **105-9** (1998), 848-849. [p.142]

[ラーデマッヘル，テプリッツ (1933)]　H.Rademacher & O.Toeplitz :『数と図形』(山崎三郎＋鹿野健訳) 日本評論社 (1989)．原著は *Von Zahlen und Figuren*, 1933. [p.43]

[リーベンボイム (1991)]　Paulo Riebenboim ：『素数の世界　その探索と発見』(吾郷孝視訳) 共立出版 (1995)．原著は *The Little Book of Big Primes*, 1991 で，*The Book of Prime Number Records*), 1988 から日本の読者向けに抜粋したもの．[p.xix, p.104]

[ルジャンドル (1798)]　A.M.Legendre ： 整数論』(*Essai sur la Théorie des Nombres*), 1798, (第 2 版，1808；補遺，1816；第 3 版，1830)．再版が Albert Blanchard，Paris から 1955 年に出版されている．[p.143]

[レニ (1947)]　A.Rényi :『偶数を素数と概素数の和に表わすことについて』(*On the representation of even numbers as the sum of a prime and almost prime*), Dokl.Akad. Nauk, SSSR, **56** (1947), p.455-458. [p.148]

[ロス (1975)]　P.M.Ross :『大きな偶数がそれぞれ p_1+p_2 か $p_1+p_2p_3$ の形をしているというチェンの定理について』(*On Chen's theorem that each large even number has the form* p_1+p_2 *or* $p_1+p_2p_3$), J. London Math. Soc. (2), **10** (1975), p.500-506. [p.148]

[ローズ (1994)]　H.E.Rose :『数論教程』(*A Cource in Number Theory*), second edition, Oxford Science Publications, 1994. [p.xix, p.132]

[ワーゴン (1990)]　S.Wagon :『編集者のコーナー：ユークリッドのアルゴリズムがまたやった』(*Editor' Corner:The Euclidean Algorithm Strikes Again*), Amer.Math. Monthly, **97** (1990), p.125-129. [p.129]

アイグナー　Martin Aigner. ベルリン自由大学数学研究所教授. ホームページは http://elib.zib.de/ICM98/Org/Committee/AignerM.html [p.114, p.128]

アダマール，ジャック　Jacques Salomon Hadamard, 1865.12.8-1963.10.17. フランス，ベルサイユに生まれ，パリに死す. 学校教育では数学以外はできが良く，ギリシア語とラテン語では優秀だったが,「7年次までは算数はビリかほとんどビリだった」と1936年に自身が語っている. その後，良い数学の教師が数学と科学に彼の気持ちを向け，エコール・ポリテクニークとエコール・ノルマル・スペリオールの入学試験までにはそれぞれに1位になった. エコール・ノルマルを選び，J. タヌリとエミール・ピカールのもとで学ぶ. 1892年にテイラー級数で定義される関数に関する論文で学位. ボルドー大学教授 (1893)，ソルボンヌの非常勤講師. コレージュ・ド・フランス (1909-1937)，エコール・ポリテクニーク教授を併任.

政治にも巻きこまれる. ドレフィス事件に積極的に参加. 第1次大戦で2人の息子を失う. ナチの台頭と共に左傾化し，1940年にフランスが占領された際アメリカに逃げ，ついでロンドンでイギリス空軍の作戦研究に加わり，1945年にパリに戻る.

18世紀に予想された素数定理を，ヴァレ・プーサンと独立に複素解析を使って証明する (1896). テイラー級数で定義された関数 (解析関数) と，その特異点の研究. 数理物理学の偏微分方程式，適切な (well-posed) 初期値問題と境界値問題の概念の導入. グリーン関数の一般化 (1932). 函数解析の基礎づけ.「汎関数」という用語の使用. 変分学.

アダマールの誕生100年記念の式典で，ローラン・シュヴァルツは次のように言っている.

「彼は彼の時代にファンタスティックな影響を与え，今あるあらゆる解析学は直接間接を問わず彼によって形作られたものであると，信じています.」[1][p.115]

アルティン Emil Artin, 1898.3.3-1962.12.20. オーストリア，ウィーンに生まれ，ドイツ，ハンブルグに死す. ライプツィヒ大学卒業 (1921). ハンブルグ大学 (1923-37, 1958-)，第 2 次大戦中アメリカに亡命し，ノートルダム大学 (1937-38)，インディアナ大学 (1938-46)，プリンストン高等研究所 (1946-58) に勤務. 現代代数学，代数的整数論，代数トポロジー，ガンマ関数論など. 非可換環論，特にアルティン環. [2] [p.xv, p.xvii, p.30]

ヴィノグラードフ Ivan Matveevich Vinogradov (Иван Матвеевич Виноградов), 1891.9.14- 1983.3.20. ロシア，ミロリューブ村 (現在プシコフ県ベリカルク) に生まれ，モスクワに死す. ペテルブルグ大学卒業 (1914). レニングラード大学教授などを経て，ソ連科学アカデミー・スチェクロフ研究所所長 (1932). 解析的整数論. ウェアリングの問題やゴールドバッハの問題などに大きな貢献 (十分大きな奇数は 3 個以下の素数の和に書けることを証明). [3] [p.xv, p.20, p.27, p.44, p.147]

ヴィーフェリッヒ Arthur Wieferich. 19 世紀末から 20 世紀初頭に活躍したドイツの数学者. ウェアリングの問題やフェルマーの最終定理に貢献. [p.144]

ウェアリング Edward Waring, 1734-1798.8.15. イギリス，シュロップシャー，オールド・ヒース (シュルーズベリの近く) に生まれ，シュロップシャー，ポンツベリに死す. ケンブリッジ大学卒業 (1857)，ロンドン，ケンブリッジ，ハンチントンの病院で医師. 1760 年からケンブリッジのルーカス数学教授職. 1770 年まで医者としても働く. 数論，代数

---

[1] 日本語の本には『数学における発見の心理』(伏見康治＋尾崎辰之助＋大塚益日古訳) みすず書房,『偏微分方程式-コーシー問題と双曲型線形偏微分方程式』現代数学の系譜 14(福原＋相澤＋山中訳・解説) 共立出版がある.

[2] 日本語の本としては,『ガロア理論入門』(寺田文行訳) 東京図書 (1974) がある.

[3] 日本語の本としては,『整数論入門』(三瓶与右衛門＋山中健訳) 共立全書 517(1969) がある.

学，代数曲線論，級数論．コーシーの比テストの発見 (1762)，対称式を基本対称式で表わすこと (1762)．ウェアリングの問題 (1770)．ウィルソンの定理 (1770)．[p.vi, p.43]

ウィルソン　John Wilson, 1741.8.6-1793.10.18. イギリス，ウェストモアランド，アップルランドに生まれ，ウェストモアランド，ケンダルに死す．

p が素数なら $1+(p-1)!$ は p で割り切れるという定理で有名． ウェアリングが最初に出版したのだが (1770)，証明はもっていなかっただろうと言われる．逆定理はラグランジュによる (1773)．[p.102]

ヴォーガン　Robert Charles Vaughan．ロンドンの王立大学数学教室の上級研究フェロー．ハーディー・リトルウッドの方法の改良，ウェアリングの問題，ゴールドバッハの問題など．ホームページは http://www.ma.ic.ac.uk/~rcv/ ． [p.145]

ウーリー　Trevor D. Wooley. ミシガン大学教授．整数論．ウェアリング問題を精力的に研究し，$G(k)$ の値の評価を改善している．ホームページは http://www.math.lsa.umich.edu/~wooley/ ． [p.145]

ヴンシュトラウム　Georg Hindenburg Wunschtraum．シレジアに生まれ，のちニュージーランドに移住. Madgeburg 大学 (1879-1885) と Jena 大学 (1885-1904) で教授．最近科学史家の M. ヴァン・ドンゲンにより，ウェアリングの問題の証明をヒルベルト以前に与えたことが発見された．[p.43]

エラトステネス，キュレネの　Eratosthenes of Cyrene, 紀元前 276-紀元前 196 頃.

北アフリカ，キュレネ (現在リビア，シャハット) に生まれ，エジプト，アレキサンドリアに死す．父はアグラオス．キュレネ，アテネで学ぶ．アルキメデスへの書簡が最近までベイルートの聖ヨセフ大学の図書館にあった．紛失はしたが，その写真は残っている．プトレマイオス 1 世から 4 世まで仕える．アレキサンドリアの図書館 (ムセイオンとよばれるミューズの神殿の中にあった) の第 3 代館長 (紀元前 245-紀元前 204，ゼノドトスの死後引き継ぐ)．あらゆる学問に通暁していたといわ

れる．主著は『プラトニクス』*Platonicus* (プラトン哲学の基礎にある数学を論じたもの) と『地理学』*Geographike*．年代学，天文学，文献学，哲学，音楽，数学，数理地理学．

素数を求めるためのエラトステネスの篩．倍積問題 (体積が倍の立方体の作図問題) を解くため機械的な道具を作る． 子午線の円弧，太陽までの距離と月までの距離を測定．ナイルの氾濫の理由の解明．[p.121, p.147]

エルデシュ Paul Erdös, 1913.3.26-1996.9.20. ハンガリー，ブダペストに生まれ，ポーランド，ワルシャワに死す．ブダペスト大学学卒業．アメリカの各地の大学に務める．数論，集合論，確率論，解析学，グラフ理論など．ベルトランの公準や素数定理の初等的解法で有名．[p.vii, p.115, p.117]

オイラー，レオンハルト Leonhard Euler, 1707.4.15-1783.9.18. スイス，バーゼルに生まれ，ロシア，サンクト・ペテルブルグに死す．ヨハン・ベルヌーイの弟子．ペテルブルグ (27-41)，ベルリン (41-66)，ペテルブルグ (66-83) のアカデミーに．66 年に全盲となるも，死ぬまで活発な研究を続ける．朴訥な人柄で，子供は 13 人．赤ん坊を抱え，子供を足元で遊ばせながら数学をしたと言われている．また，お茶をすすりながら孫と話をしているとき，突然に死んだという．

数学史上最大の多作家．ケーニヒスベルクの橋を一筆書きする問題や多面体の面·辺·頂点の数の関係式 (オイラー標数) で，グラフ理論とトポロジーの祖となる．フランスの物理学者アラゴー (1786.2.26-1853.10.2) は，オイラーを「解析学の化身」と称え,「人が息をするように，鷲が空を舞うように，オイラーは計算をした」と言っている．[p.vi, p.27, p.101, p.103, p.104, p.109, p.112, p.114, p.146]

ガウス，カール・フリードリヒ Johann Carl Friedrich Gauss, 1777.4.30-1855.2.23. ブルンシュヴィク公国，ブルンシュヴィク (現在ドイツ領) に生まれ，ハノーバー，ゲッティンゲン (現在ドイツ領) に死す．

ゲッティンゲン天文台長 (30 才)，ゲッティンゲン大学教授 (31 才)．数学上の伝説は数多く，どれを省くこともできないので，すべて省略．

ただし，正 17 角形の作図可能性の発見は，彼が数学に献身するきっかけでもあり，自分の墓に刻んで欲しいと願ったことだけ (実際には刻まれなかったが) 述べておく．

パトロンのブルンシュヴィク公爵がプロシャとの戦争で死ぬまでは，家庭的にも恵まれていたが，その後ゲッティンゲンに移り (1807)，父をなくし，妻を次男のお産でなくし，その子もすぐに死んでいる．その後は家庭的には恵まれなかったと言われる．

1801 年 1 月 1 日に G. ピアッツィ(1746.7.16-1826.7.22) によって発見された小惑星ケレスは 6 週間追跡観測されたが，太陽の位置との関係で見失われてしまった．ガウスはこの軌道を計算するため，3 回の観測だけで小惑星の軌道を素早く計算する方法を開発し，発表した (1809)．ガウスは自分の計算による予測をゴータ天文台のツァハに送り，1802 年 1 月予測した位置の近くで H.W.M. オルバース (1758.10.11-1840.3.2) によって発見された．

1831 年以降ウェーバーと共同で電気と磁気の研究をし，電磁気通信機を発明した．[4][p.v, p.102, p.115, p.134]

ギャロット　Yves Gallot, 1966-. フランス，ツールーズに生まれ，今も住んでいる．高等電気学校 (l'Ecole Supérieure d'Electricité) の技術者．コンピュータ整数論．多くの大きな素数の発見者．ホームページは http://www.utm.edu/research/primes/programs/gallot/ ．[p.122]

ケンプナー　A.J.Kempner. ドイツの数学者．ウェアリングの問題に貢献．[p.44]

コーシー　Augustin Louis Cauchy, 1789.8.21-1857.5.23. パリに生まれ，(パリ近郊) ソーに死す．エコール・ポリテクニーク (1807) と土木学校 (1810) 卒業．エコール・ポリテクニーク教授．少年時，革命直後のパリを避けてアーキュイユに疎開していたコーシー家を訪れたラグラ

[4]日本語の本に『ガウス整数論』(1801)(高橋正仁訳) 朝倉書店,『誤差論』(飛田武幸，石川耕春訳) 紀伊国屋書店がある．伝記や業績については，ダニングトン『ガウスの生涯』(銀林浩＋小島穀男＋田中勇訳) 東京図書，G. ギンディキン『ガウスが切り開いた道』(三浦伸夫訳) シュプリンガー・フェアラーク東京，高橋正仁『ガウスの遺産と継承者たち』海鳴社などがある．

ンジュに，指導を受ける．本格的に数学を勉強する前に古典語をみっちりと学ぶようにと忠告を受け，13 才から 2 年間語学に没頭．

『解析学教程』(1821) など，これ以降の教科書の典型となるものを幾つも出版．業績は幅広く，特に収束級数論，複素関数論，微分方程式論などの基礎付けなど．[p.143]

コールドウェル　Chris Caldwell, 1956-. アメリカ，テネシー大学マルチン分校教授．1984 年に，カルフォルニア大学バークレイ校で PhD を取得．素数に関するホームページを管理している．彼のホームページは http://www.utm.edu/~caldwell . [p.122]

ゴールドバッハ　Christian Goldbach, 1690.3.18-1764.11.20. プロシャ，ケーニヒスベルク (現在ロシア，カリーニングラード) に生まれ，ロシア，モスクワに死す．1725 年セント・ペテルスブルグの数学と歴史の教授となり，1728 年モスクワに行き，ピョートル II 世の家庭教師となる．ヨーロッパを遍歴し，多くの数学者と会う．整数論での仕事が重要で，主にオイラーとの文通の中で公表される．1724 年のオイラーへの手紙の中で，有名な予想 (偶数に対するもの) が述べられている．[p.vi, p.146]

ゴールドマン　Jay R. Goldman. ミネソタ大学教授．[p.xix]

ザギエ　Don B. Zagier, 1951.6.29-. ボン大学卒業 (1971) 後，インド，中国，日本で働く．九州大学の教授だったことがある．代数幾何，数論．[p.128]

シェルク　Peter Scherk, 1910-1985. トロント大学教授．代数学，整数論．[p.xv, p.30]

シドロフスキー　Andrei Borisovich Shidlovskii(Андрей Борисович Шидловский), 1915.8.13-. アラティール (その後チェコスロバキア共和国領) の生まれ．ソ連の数学者．モスクワ大学卒業 (1950)．モスクワ大学の数論講座担当 (1954)，教授 (1960)．超越数論．[p.xi, p.4]

シューア　Issai Schur, 1875.1.10-1941.1.10. ベラロシア，モギリョフに生まれ，パレスチナ，イェルサレムに死す．13 歳でラトヴィアに行き，1894 年ベルリン大学に入学し，フロベニウスに学ぶ．ボン大学，ベル

リン大学教授 (1913). 1939 年ナチの迫害のためパレスチナに亡命.

表現論，数論，ガロア理論，有限群論，行列論，直交関数系理論. シューアの補題，シューア関数. [p.144]

シュニレルマン Lev Genrikhovich Shnirelman (Лев Генрихович Шнирельман), 1905.1.15-1938.9.24. ベロロシア，ゴメリに生まれ，ソ連，モスクワに死す. モスクワ大学に 16 歳で入学し，1925 年卒業. ヒンチン，ルージン，ウリゾーンに学ぶ. 1934 年以後モスクワ大学および科学アカデミー研究所に勤務. 整数論，代数学，トポロジー，変分法の位相的方法. 3 閉測地線に関するポアンカレの問題を解く (リュステルニク・シュニレルマンの定理). ゴールドバッハの予想の解法に本質的な進展 (任意の自然数は 20 個以下の素数の和に書けることを証明). [p.xv, p.18, p.106]

シュライヤー Otto Schreier, 1901.3.3-1929.6.2. オーストリア，ウィーンに生まれ，ドイツ，ハンブルグに死す. 1920 年ウィーン大学に入学し，1923 年 11 月 8 日に群拡大の理論で学位取得. その後 28 才で病死するまでハンブルグ大学に在職. フルトヴェングラーとライデマイスターの影響を強く受ける. 結び目群の研究など. [p.xvii]

ジラール，アルベール Albert Girard, 1595-1632.12.8. フランス，サン・ミイール (St Mihiel) に生まれ，オランダ，ライデンに死す. フランスから宗教上の理由でオランダに亡命. ライデン大学教授.

代数学の基本定理を初めて述べ，$0, \sqrt{-1}$, 負の指数の公然とした使用. 球面三角形の面積を求める. $\sin, \cos, \tan$ という省略記号を初めて使う (1626). [p.20]

セール Jean Pierre Serre, 1926.9.15-. フランス，バジュの生まれ. エコール・ノルマル・シュペリオール卒業 (1948). コレージュ・ド・フランス教授 (1956-). 代数幾何学，代数トポロジー. 1954 年にフィールズ賞受賞. [5][p.132]

セルバーグ Alte Selberg, 1917.6.14-. ノルウェー，ランゲスーンの生ま

[5] 日本語の本に,『有限群の線形表現』『数論講義』岩波書店,『ガロア理論特論』トッパンなどがある.

れ．オスロ大学卒，教授．プリンストン高等数学研究所教授．整数論，解析関数論，表現論など．1950 年フィールズ賞受賞．[p.115, p.148]

ダヴェンポート Harold Davenport, 1907.10.30-1969.6.9. イギリス，ランカシャー，ハンコートに生まれ，ケンブリッジシャー，ケンブリッジに死す．リトルウッドの弟子．コクセターの友人．ロンドン大学 (1945)，ケンブリッジ大学教授 (1958)．[p.145]

チェビシェフ Pafnuty L'vovich Chebyshev, 1821.5.16-1894.12.8. ロシア，オカトヴォに生まれ，セント・ペテルスブルグに死す．モスクワ大学卒 (1841)．ペテルブルグ大学 (1847-82)，ペテルブルグ科学アカデミー (1859) で働く．確率論，数論，関数近似論，集合論など．弟子も多数．[p.116]

チェン Jing-Run Chen(陳景潤), 1933-. 整数論．双子素数の問題，ウェアリングの問題 ($g(5) = 37$) やゴールドバッハの問題に貢献 (1973)．[p.44, p.121]

ツィーグラー Günter M. Ziegler．ベルリン工科大学数学教室教授．ホームページは http://www.math.tu-berlin.de/ ziegler/ [p.114, p.128]

ディオファントス，アレキサンドリアの Diophantos = Diopantus, 246?-330? (200?-284?)．アレキサンドリアに住んでいたことがあることしか分らない．他には 33 才で結婚し，息子が 42 才で死んだ時から 4 年後 84 才で死んだということが解答である算術の問題が残っており (5 ないし 6 世紀の『古代ギリシャ詩華集』)，生没年そのものはまったくあてにならないのだが，84 年間生きていただろうということにはなっている．

『算術』全 13 巻．代数学の初歩と不定方程式を論じる．前半の 6 巻のみ現存．アラビア語を介し，1575 年に初めてラテン語に翻訳された．1621 年発行のバシェ·ド・メリジアク訳のラテン版訳の余白にフェルマーが書き込みをする．その他多角数に関する断片が残存している．[p.18, p.140]

ディクソン Leonard Eugene Dickson, 1874.1.22-1954.1.17. アメリカ，アイオワ州，インデペンデンスに生まれ，テキサス州，ハーリントンに

死す．テキサス大学卒業 (1893)．シカゴ大学教授 (1900-39)．数論，群論，有限体上の一般線形群の理論．[p.136, p.145]

ディリクレ　Peter Gustav Lejeune Dirichlet, 1805.2.13-1859.5.5. フランス帝国，デューレン (現在はドイツ) に生まれ，ハノーバー，ゲッティンゲン (現在はドイツ) に死す．長くベルリン大学 ('28-55)，ゲッティンゲン大学教授 (ガウスの後任)．算術級数定理，現代的な関数の定義，ディリクレ問題，フーリエ級数論，フェルマー予想の部分的解決．[6] [p.111, p.127, p.147]

ドゥ・ラ・ヴァレ・プーサン　Charles Jean Gustave Nicolas de la Vallée Poussin, 1866.8. 14-1962.3.2. ベルギー，ルーヴァンに生まれ，ルーヴァンに死す．ルーヴァン大学教授 (1897)．1896 年にアダマールと異なる方法で素数定理を証明．微分方程式やリーマンのゼータ関数の理論でも貢献.『解析教程』は有名．[p.115]

テプリッツ　Otto Toeplitz, 1881.8.1-1940.10.11. ドイツ，ブレスラウ (現在ポーランド，ブロツラフ) に生まれ，イェルサレム (当時イギリス統治下) に死す．ヒルベルトの助手，キール大学，ベルリン大学教授．1933 年ナチにより免職され，1938 年イェルサレムに移住．積分方程式論，無限変数の関数論，線形代数，数学史，数学教授法．テプリッツ行列．[p.43]

ナゲル　Trygve Nagell, 1895.7.13-1988. ノルウェー，オスロに生まれ，スウェーデンのウプサラに死す．オスロ大学卒業後 (1920)，オスロ大学の教員となり，助教授 (1930-31)．スウェーデンのウプサラ大学教授 (1931-1962)．

整数論，抽象代数．特に，不定方程式，代数的数，環論に業績．[p.xix]

ニコマコス，ゲラサの　Nicomachus of Gerasa, 60 年頃-120 年頃．ローマ帝国，シリア属州，ゲラサ (パレスティナ) の生まれ．その『算術入門』は初めて算術を幾何とは独立の教科として著したもの．以降 1000 年以上にも亘って，算術の標準的な教科書となる．ギリシャ数字でな

---

[6] 日本語の本に『ディリクレ・デデキント　整数論講義』(酒井孝一訳・解説) 現代数学の系譜 5 共立出版がある．

く，アラビア数字を使っている．[p.139]

ハウスドルフ　Felix Hausdorff, 1869.11.8-1942.1.26. ドイツ，ブレスラウ (現在ポーランド領) に生まれ，ボンに死す．ライプツィッヒ大学卒業後ライプツィッヒ大学に勤め (1891)，後ボン大学へ (1910)．途中ゲッティンゲンに招かれたが，断っている．ナチスの迫害に遭い，収容所に送られることを拒んで妻とともに自殺.

位相空間論，距離空間論，半順序集合など．ハウスドルフ空間. [p.144]

パスカル　Blaise Pascal, 1623.6.19-1662.8.19. フランス，オーベルジュ，クレルモン (現在クレルモン・フェラン) に生まれ，パリに死す．父エチエンヌ・パスカル (1588.5.2-1651.9.24)，リマソン (蝸牛線) の発見者. 命名はロベルヴァルによる) は裕福な家系で，息子の教育のためパリに移住 (1631)．父に伴われ，メルセンヌ・アカデミーに参加. ジラール・デザルグ (1593-1662) に会い，その射影幾何学を発展させたのは，アポロニウスの理論の拡張でもある (パスカルの定理=神秘 6 角形の定理『円錐曲線私論』(1640))．実用面での発明も多く，今も普通に使われている手押し一輪車も彼の発明．パスカル式車輪 (=手回し計算機,1640) も人気があり，8 台が現存している．1646 年末にトリチェリの真空実験の噂を聞き，流体の静力学について考察．特に空気を流体として考察する点が新しく，高度による気圧の差を予言 (『液体の平衡に関する大実験談』).

サイコロ賭博の賭金分配に関する問題に与えたパスカルの解が論争をよび，1654 年 7 月 29 日-10 月 27 日までフェルマーと文通して意見を交換する中で確率論が成立する．1658 年の春の一夜激しい歯痛に悩まされ眠れぬパスカルは，サイクロイドに関するメルセンヌの未解決問題を考察することを思いつき，夜明けまでに問題を解いたときには歯痛が治まっていたという．この時解いた問題はすでに初等的には解けない問題で，本質的には三角関数の微積分が必要な問題であった．しかし彼は自分流の代数言語を作りだし，それによって式を書かずに答えを得ている．パスカルの言語はとりわけ明晰で，代数記号法の使用をなぜ拒むか分からぬときでさえその力業には感嘆するばかりだと，ブルバキも書い

ている．天才にしか使えないものでなく，凡人にも使えるようにするために記号が考案されたときが，微積分の成立ということになる．

ポール・ロワイヤルに入ってイエズス会と論争．『パンセ』．体の弱かった彼が 40 才前まで生きられたのは，それでも考える葦だったためかもしれない．[7] [p.119]

ハーディー Godfrey Harold Hardy, 1877.2.7-1947.12.1. イギリス，サレイ，クランレイに生まれ，ケンブリッジシャー，ケンブリッジに死す．ケンブリッジ大学出身．ケンブリッジ大学 (1909-19)，オックスフォード大学教授 (1919-42)．整数論，関数論．リトルウッドとの共同研究が多く，ラマヌジャンを援助したことでも知られる．彼の数学に対する考え方ははっきりしていて

「数学者のパターンは，画家や詩人と同様，美しくなければならないし，アイデアは，色や言葉と同様，調和した適合がなければならない．美こそが最初のテストであり，醜い数学に恒久的な場などないのだ.」と言っている．[8][p.xv, p.44, p.145, p.147]

ヒルベルト David Hilbert, 1862.1.23-1943.2.14. プロシャ，ケーニヒスベルク (現在ロシア領，カリーニングラード) に生まれ，ドイツ，ゲッティンゲンに死す．ケーニヒスベルク大学教授 ('90)，ゲッティンゲン大学教授 ('95)．A. フルヴィッツ，H. ミンコフスキーと親交．1900 年パリの国際数学者会議での 23 の問題は，20 世紀も終わりに近づいて，ほとんど解決され，更なる発展を遂げている．ちょうど 1 世紀ほどで解けてしまうというのは程がよい．彼が解くことを選ばなかったフェルマー予想も解けてしまい，数学者以外に説明できる問題が少なくなった．また，基底定理は当時の不変式論の大家ゴルダンに「これは数学ではない．神学だ.」と言わせている．現代数学への一つの里程標である[9]．

---

[7]日本語では人文書院の『パスカル全集』，教文館の『パスカル著作集』，中央公論社の『パスカル』世界の名著 24 があり，科学論文を含めてほとんどの著述が翻訳されている．また『パンセ』筑摩世界文学大系の他にも種々の文庫本が出版されている．

[8]日本語の本に『ある数学者の生涯と弁明』(柳生孝昭訳) シュプリンガー数学クラブがある．

[9]日本語に訳されているものも多く，S. コーン-フォッセンと共著『直観幾何学』(芹沢正三訳) みすず書房,『数学の問題－ヒルベルトの問題』(一松信訳・解説) 現代数学の系譜 4 共立

[p.xv, p.43, p.143]

ピュタゴラス，サモスの　Pythagoras of Samos, 紀元前 570-501 (572?-492?, 580?- 500?, 582- 493 など諸説あり)．イオニア，サモスに生まれ，リュカニア，メタポンタムに死す．数学・哲学者．前 532 年頃南イタリア，クロトンに移住．哲学・宗教集団を創始．この学派の数学への貢献は大きい．明けの明星と宵の明星が同じ星であることを見つけた．「万物は数である．」[p.vi, p.138]

ヒンチン　Aleksandr Yakovlevich Khinchin(Александр Яковлевич Хинчин), 1894.7.19-1959.11.18. ロシア，カルージュスカヤ・グベルニヤ，コンドゥロヴォに生まれ，ソビエト連邦，モスクワに死す．モスクワ大学卒業 (1916)，モスクワ大学教授 (1927)．関数論，整数論 (ハーディー-リトルウッドの結果を強化)，確率論 (大数の法則の拡張，確率過程)，ディオファントス近似，連分数の測度論など．情報理論の数学的基礎や統計力学の基礎づけなど，著書も多い．本文の著者．[p.vi]

ファン・デル・ヴェルデン　Bartel Leendert van der Waerden, 1903.2.2-1996.1.12. オランダ，アムステルダムに生まれ，スイス，チューリッヒに死す．アムステルダム大学とゲッティンゲン大学に学ぶ (1919-25)．フローニンゲン大学，ライプツィッヒ大学 (1931) で働くも，外国籍のためナチの迫害に遭う．戦後しばらくシェル石油で応用数学者として働き，1947 年ジョン・ホプキンス大学へ，1948 年アムステルダム大学に戻り，1951 年からチューリヒ大学教授．1924 年当時はエミー・ネーターのもとで学ぶ．代数幾何学 (代数多様体の次元の定義)，量子力学や数理統計学への群論の応用など幅広い．ガロア理論では，ほとんどすべての整係数の代数方程式のガロア群が対称群になることを示す．ネーター学派の代数学の集大成としての『(現代) 代数学』(1930) は重要．数学史，物理科学史，古代科学史などにも著書がある．[10] [p.xv, p.xvii, p.8]

出版,『幾何学の基礎』(寺阪英孝＋大西正男訳・解説) 現代数学の系譜 7 共立出版 (1970)，P. ベルナイスと共著『数学の基礎』(吉田夏彦＋渕野昌訳) シュプリンガーフェアラーク東京，アッケルマンと共著『記号論理学の基礎』(伊藤誠訳) 大阪教育図書 (1954)，R. クーラントと共著『数理物理学の方法　全 4 巻』(齋藤利弥監訳，丸山滋弥訳) 東京図書 (1959-62) などがある．

フェルマー　Pierre de Fermat, 1601.8.20 (17) - 1665.1.12. フランス，(トゥールーズ近くの) ボーモン・ド・ロマーニュに生まれ，カッストルに死す．オルレアン大学で法律を学び，トゥールーズ高等法院参与．数論以外にも，具体的な関数に関する微積分や確率論の創始などがある．最近まで予想であった最終定理はあまりにも有名．[p.vi, p.18, p.81, p.90, p.101, p.103, p.125, p.127]

フルヴィッツ　Adolf Hurwitz, 1859.3.26-1919.11.18. ドイツ，低地サクソン，ヒルデスハイムに生まれ，スイス，チューリッヒに死す．始めシューベルトに学び，ベルリン大学で，クンマー，ワイエルシュトラス，クロネッカーの講義を受ける．F. クラインとライプツィッヒに移り，彼のもとでモデュラー関数に関する博士論文．ケーニヒスベルク大学 (1884-92) でヒルベルト，ミンコフスキーを教え，長く親交．フロベニウスの後任として，チューリッヒ工科大学教授 (1892).

実係数方程式の根の実部がすべて負になる条件を求めるのをフルヴィッツの問題という．多元数論，e の超越性の証明の簡易化 (1853)，等周問題の三角級数による美しい解答 (1901)．[11][p.18, p.143]

ブルーデルン　Jörg Brüdern. ドイツ，シュトゥットガルト大学教授．ホームページは http://www.mathematik.uni-stuttgart.de/mathA/lst4/bruedern.html. [p.145]

ブルン　Viggo Brun, 1885.10.13-1978.8.15. ノルウェー，リールの生まれ．オスロ大学教授．数論．ブルンのふるい．[p.121, p.147]

ベイカー　Alan Baker, 1939.8.19-. イギリス，ロンドンの生まれ．ケンブリッジ大学トリニティ・カレッジで学位 (1964)，フェローの後 1974 年に教授．1970 年ニースの国際数学者会議でフィールズ賞受賞，数論

[10] 日本語に訳されているものも多く，『現代代数学 1,2,3』(銀林浩訳)，東京図書 (1959，原書は 1937 の第 2 版)，『代数幾何学入門』(前田博信訳)，シュプリンガー・フェアラーク東京 (1994，原書は 1939)，『数学の黎明－オリエントからギリシャへ』(村田全＋佐藤勝造訳) みすず書房 (1984，原書は 1954)，『代数学の歴史－アル-クワリズミからエミー・ネーターへ』(加藤明史訳) 現代数学社 (1994，原書は 1985) などがある．

[11] 日本語に訳されたものに，文献表にある R. クーラントとの共著の『楕円関数論』がある．

特にディオファントス方程式の研究で．ヒルベルトの第7問題の解決．超越数論．[p.xix]

ベルトラン Joseph Louis François Bertrand, 1822.3.11-1900.4.3. フランス，パリに生まれ，パリに死す．エコール・ポリテクニク卒 (1839). エコール・ポリテクニク (1856-)，エコール・ノルマル，コレージュ・ド・フランス (1862-) の教授．1878 年で一旦教えるのは止めたが，8 年後にまた教えはじめる．

数論，確率論，微分幾何など．ベルトランの仮説 (1845，証明はチェビシェフ (1850) による)．ベルトランの逆説 (1888 年の確率論の教科書で述べた)．ガウスの『誤差論，最小自乗法』のフランス語訳．著書も多く，語り口は魅力的だが，誤りもあり厳密さに欠ける点があった．[p.116]

ポアンカレ，アンリ Henri Poincaré, 1854.4.29-1912.7.17. フランス，ナンシーに生まれ，パリに死す．エコール・ポリテクニーク (1873-) の後鉱山学校に学び C. エルミートに師事し，1879 年に学位取得．ソルボンヌ大学数理物理学教授 (1881-死)．微分方程式論，保型関数論，天体力学．代数トポロジーと多変数関数論の創始者．最後の万能の人とよばれる．啓蒙活動も重要[12]．[p.43]

マン Henry Berthold Mann, 1905.10.2-. アメリカの数学者．代数学，整数論，数理統計学．[p.xv, p.18, p.30]

メレ E. Maillet. 19 世紀末から 20 世来はじめに活躍したフランスの数学者．代数学，整数論．[p.136, p.143]

ヤコビ Carl Gustav Jacob Jacobi, 1804.12.10-1851.2.18. プロイセン，ポツダム (現在ドイツ領) に生まれ，ドイツ，ベルリンに死す．ユダヤ人銀行家の家に生まれ，ベルリン大学卒業後，教授資格取得のためキリスト教に改宗．ケーニヒスベルク大学に招かれ (1826)，教授 (1832) に．1843 年健康上職を辞し，イタリヤへ．1844 年帰国後ベルリン大学教授．

[12] 日本語の本は『常微分方程式-天体力学の新しい方法-』(福原満州雄＋浦太郎訳・解説) 現代数学の系譜 6，共立出版 (1970) があり，岩波文庫には『科学と仮説』『科学と方法』『科学の価値』『科學者と詩人』『晩年の思想』がある．

力学，微分幾何，線形代数学，整数論，変分法，微分方程式論，楕円関数論など．ヤコビのテータ関数．ヤコビアン，ハミルトン・ヤコビの方程式．数学教授法としてのセミナー形式を考案．[p.18, p.136]

ユークリッド ＝ エウクレイデス，アレキサンドリアの Eucleides = Euclid of Alexandria = ΕΥΚΛΕΙΔΟΥ，紀元前 330?-275?(365?-300?)．エジプト，アレキサンドリアの生まれ．プラトンのアカデミアに学ぶ．

単に『原論』と言えば彼の『幾何学原論』のこと．古代ギリシャ数学の集大成であるばかりでなく，その後 2000 年間の数学のあり方，数学教育のあり方に最大級の影響を及ぼした作品である．結果がオリジナルでないという非難をする人もあるが，叙述の仕方こそが彼の業績であり，そのことが最も大きな影響を与えたものである．また，幾何学以外にも著作は多い．『補助論』,『図形分割論』,『光学』など残っているものもあるが (ハイベルグの著作中に見いだされる),『焦面』,『不定命題』,『円錐曲線 (アポロニウスの結果をまとめたものらしい)』,『間違った結論について (詭弁論か?)』,『音楽理論』,『諸現象 (天文学)』など失われたものが多い．

アレキサンドリアでプトレマイオスＩ世に「幾何学に王道はない」と言った言葉は数学者にとっては誇りであるが．[p.109]

ライト Elizabeth Maitland Wright．イギリス，アバディーン大学教授．[p.xix]

ラグランジュ Joseph-Louis Lagrange, 1736.1.25-1813.4.10．サルディニア・ピエモン，トリノ (現在イタリア領) に生まれ，パリに死す．トリノ王立砲兵学校数学教授 (1755)，オイラーの後任としてフリードリヒ大王に招かれ，ベルリン科学アカデミー数学・物理学主任に ('66-86)．翌年ルイ 16 世の招きで，パリへ (1787)．パリの科学アカデミー会員となる．エコール・ポリテクニーク初代校長 (1794)．メートル法制定委員長．解析学，整数論，解析力学 (力学を解析学の 1 分野に変える)．群論の萌芽としての置換の研究．

フランス革命を生き残り，化学者ラヴォアジェがギロチンに消えたと

き,「この頭を落すには一瞬しか掛からないが，このような頭脳が生まれるのには百年でも足らない.」と語った. [p.18, p.104, p.132, p.143]

ラーデマッヘル　Hans Rademacher, 1892.4.3-1969.2.7. ドイツ，シュレジッヒ・ホルシュタイン，ヴァンシュベクに生まれ，アメリカ，ペンシルヴァニア，ハーヴァーフォードに死す．変分法をカラテオドリに学び，数論をランダウに学んだ．ベルリン，ハンブルグ，ブレスラウ大学で教えていたが，平和主義者のため 1933 年ドイツを逐われ，アメリカに移住する．ペンシルヴァニア大学教授定年 (1962) 後は，ニューヨークのロックフェラー研究所．実関数論，直交級数論，数論．分割関数の増大の漸近公式で有名．[p.43]

ランダウ　Edmund Georg Herman Landau, 1877.2.14-1938.2.19. ドイツ，ベルリンに生まれ，ベルリンに死す．ベルリンにあるフランスのリセを 2 年少なく 16 才で卒業後，ベルリン大学で数学を学ぶ．フロベニウスの指導のもと，1899 年に整数論で学位．数学パズルにも興味をもち，学位取得の前にもチェスについての数学理論の本を 2 冊書いている．1901 年に教授資格を得ているが，その際フロベニウスはランダウの仕事に，リーマン予想が証明されてしまったら (1999 年現在証明されていないが) 重要さを失うという理由で，批判的であったという．

ベルリン大学 (1899-1909) で教え始めて，1904 年には自分の年 (27) より著書の数が多くなる．教授能力に目覚める．初心者コース，自分の専門の数論，数学の基礎，無理数論，集合論などの講義をする．1909 年にミンコフスキーの後任としてゲッティンゲン大学教授 (-33) になる．1913 年に F. クライン隠退後の後任問題がこじれる．カラテオドリ，ヘッセが就任したがすぐに転出．ランダウはユダヤ人のシューアを押したが，クーラントに決まる．その後，ナチ政権に大学を追われ，オランダに亡命，ケンブリッジ大学 (1935-1937)，ブリュッセル大学 (1937-).

主な業績は解析的整数論と素数分布．1896 年のヴァレ・プーサンとアダマールの素数定理の証明を大幅に簡略化 (1903 年)．解析的数論の始めての系統的な書物と 1 変数解析関数論の書物も重要．[p.18, p.28, p.117, p.146]

リウヴィル　Joseph Liouville, 1809.3.24-1882.9.8. フランス，サン・オマーに生まれ，パリに死す．エコール・ポリテクニーク教授 (1833)．e の超越性，代数学の基本定理の証明の簡単化．積分方程式のスツルム–リウヴィル理論．純粋応用数学雑誌 (リウヴィル誌) の刊行 (1836)．ガロアの論文を整理し，この雑誌に掲載してから，ガロアの業績が世に知られるようになった．経度局員 (1862)．[p.138, p.143]

リトルウッド　John Edensor Littlewood, 1885.6.9-1977.9.6. イギリス，ケント，ロチェスターに生まれ，ケンブリッジシャー，ケンブリッジに死す．ケンブリッジ大学，トリニティ・カレッジに学ぶ (1907 卒)．マンチェスター大学 (1907-10)，トリニティ・カレッジ (1910-，教授 1928-50)．G.H. ハーディーとの共同研究 (35 年間) で，級数，リーマンのゼータ関数，不等式，関数の理論などに成果．[13][p.xv, p.44, p.145, p.147]

リニク　Yurii Vladimirovich Linnik(ЮрийВладимирович Линник), 1915.1.21-1972.6.30. ウクライナ，ベラヤ・ツエルコフに生まれ，ソ連，レニングラードに死す．レニングラード大学卒 (1938)，教授 (1944)．数論，確率論，数理統計学．中心極限定理の情報理論的証明．整数論における大きなふるいの方法．3 素数のゴールドバッハ予想のヴィノグラードフの定理の新証明．ウェアリングの問題の初等的証明 (1924) [p.xv, p.44]

リフシッツ　Henri Lifchitz, 1948-. パリ生まれの電子工学者．$\pi(n)$ やフィボナッチ数，ルーカス数に関心．1971 年に 20×10^6 までの素数表を出版．現在 (1999 年) の，最大の双子素数の発見者．ホームページは http://ourworld.compuserve.com/homepages/hlifchitz/ である．[p.104, p.122]

リーマン　Georg Friedrich Bernhard Riemann, 1826.9.17-1866.7.20. ハノーバー，ブレセレンツ (ダンネベルクの近く) に生まれ，イタリア，セラスカに死す．ゲッティンゲン大学教授 (1859-)．1862 年肺結核にかかり，その後療養のため大半をイタリアで過ごす．

[13] [訳註] 日本語の本に『リトルウッドの数学スクランブル』(金光滋訳) 近代科学社 (1990) がある．

リーマン多様体 (幾何学)，リーマン積分，リーマン・ゼータ関数 (リーマン予想)，リーマン面．リーマンの名に触れずに現代数学を語ることは難しい． [p.115]

ルジャンドル　Adrian Marie Legendre, 1752.9.18-1833.1.10. パリに生まれ，パリに死す．パリのコレージュ・マザランで学ぶ．ダランベールの推薦でパリの陸軍士官学校で教える (1775-1780)．科学アカデミー (会員 1783-1793)．エコル・ポリテクニーク教授 (1816-)．経度調査局員 (1818-33).『整数論』,『楕円関数論』はよく読まれた．フェルマー予想の部分的解決．40 年以上平行線の公準を証明しようとした．[p.96, p.143]

M.A. ルコムスカヤ　M.A.Lukomskaya=M.A.Лукомская. [p.9]

ワーゴン　Stan Wagon. アメリカ，スミス大学数学科教授． [p.129]

索引

著　者
ア・ヤ・ヒンチン（Aleksandr Yakoblevich Khinchin）

1894年　ロシア，コンドゥロヴォ生まれ．
1916年　モスクワ大学卒業
1927年　モスクワ大学教授
1959年　モスクワに死す

訳・解説者略歴
蟹江幸博（かにえ・ゆきひろ）

1976年　京都大学大学院理学研究科博士課程修了
現　在　三重大学教育学部教授

主な訳書　V.I. アーノルド『古典力学の数学的方法』（共訳，岩波書店）
V.I. アーノルド『カタストロフ理論』（現代数学社）
E. ハイラー，G. ワナー『解析教程上・下』（シュプリンガー・フェアラーク東京）
G. トス『数学名所案内上・下』（シュプリンガー・フェアラーク東京）
J.W. ミルナー『微分トポロジー講義』（シュプリンガー・フェアラーク東京）

ホームページ
http://www.com.mie-u.ac.jp/~kanie/tosm/

はじめよう数学 4

数論（すうろん）の 3 つの真珠（しんじゅ）

●――――2000年 9 月10日　第 1 版第 1 刷発行

著　者――ア・ヤ・ヒンチン
訳・解説者――蟹江幸博
発行者――大石　進
発行所――株式会社 日本評論社
〒170-8474 東京都豊島区南大塚3-12-4
電話 03-3987-8621（販売）-8599（編集）
振替 00100-3-16
印刷所――三美印刷株式会社
製本所――株式会社 難波製本

装幀／駒井佑二
ISBN4-535-60843-1　Printed in Japan

はじめよう数学